Information in the US-CERT Cyber Security Bulletin is a compilation and includes information published by outside sources, so the information should not be considered the result of US-CERT analysis. Software vulnerabilities are categorized in the appropriate section reflecting the operating system on which the vulnerability was reported; however, this does not mean that the vulnerability only affects the operating system reported since this information is obtained from open-source information.

This bulletin provides a summary of new or updated vulnerabilities, exploits, trends, viruses, and trojans. **Updates to items appearing in previous bulletins are listed in bold text.** The text in the Risk column appears in red for vulnerabilities ranking High. The risks levels applied to vulnerabilities in the Cyber Security Bulletin are based on how the "system" may be impacted. The Recent Exploit/Technique table contains a "Workaround or Patch Available" column that indicates whether a workaround or patch has been published for the vulnerability which the script exploits.

- **Multiple Vendors Samba smbd Security Descriptor (Updated)**
- **Multiple Vendors Squid NTLM fakeauth_auth Helper Remote Denial of Service (Updated)**
- Multiple Vendors LibXPM Bitmap_unit Integer Overflow
- Multiple Vendors XLI Internal Buffer Management
- Multiple Vendors XLoadImage Compressed Image Remote Command
- **Open Group Motif / Open Motif libXpm Vulnerabilities (Updated)**
- OpenBSD copy(9) Function
- RedHat Linux Remote Buffer Overflow
- **Remote Sensing LibTIFF Two Integer Overflow Vulnerabilities (Updated)**
- **Rob Flynn Gaim Multiple Remote Denials of Service (Updated)**
- HTTP Anti Virus Proxy Virus Detection
- **Squid Proxy FQDN Remote Denial of Service (Updated)**
- Sun Solaris AnswerBook2 Multiple Cross-Site Scripting
- Symantec Enterprise Firewall DNSD DNS Cache Poisoning
- The PaX Team PaX Undisclosed Arbitrary Code Execution
- Trolltech QT Arbitrary Code Execution
- **University Of Washington IMAP Server CRAM-MD5 Remote Authentication Bypass (Updated)**
- **Vim Insecure Temporary File Creation (Updated)**
- **XFree86 XDM RequestPort False Sense of Security (Updated)**

- Multiple Operating Systems
  - **Apache mod_python Information Disclosure Vulnerability (Updated)**
  - **Appalachian State phpWebSite Arbitrary Code Execution Vulnerability (Updated)**
  - auraCMS Discloses Path to Remote Users and Permits Cross-Site Scripting Attacks
  - Aztek Forum Information Disclosure Vulnerability
  - Bfriendly.com Einstein Information Disclosure Vulnerability
  - Carsten's 3D Engine Remote Code Execution Vulnerability
  - COINSoft Technologies phpCOIN Input Validation Vulnerabilities
  - Computer Associates License Remote Code Execution Vulnerability
  - demof Forumwa Input Validation Vulnerabilities
  - D-forum Input Validation Vulnerabilities
  - Drupal Unspecified Cross-Site Scripting Vulnerability
  - Ethereal Buffer Overflow
  - Foxmail Remote Code Execution Vulnerability
  - GNU 427BB Input Validation Vulnerabilities
  - GNU CuteNews Input Validation Vulnerabilities
  - **GNU Gaim Denial of Service Vulnerability (Updated)**
  - GNU ProjectBB Input Validation Vulnerabilities
  - GPL MercuryBoard SQL Injection and Script Insertion Vulnerabilities
  - **GPL MyPHP Forum SQL Injection Vulnerability (Updated)**
  - Hewlett-Packard OpenVMS Access Vulnerability
  - Jason Hines PHPWebLog Remote File Include
  - **Mozilla / Firefox / Thunderbird Multiple Vulnerabilities (Updated)**
  - **Mozilla Browser and Mozilla Firefox Remote Window Hijacking (Updated)**
  - **Mozilla Firefox Remote Code Execution Vulnerability (Updated)**
  - **Mozilla Firefox Multiple Vulnerabilities (Updated)**
  - **Mozilla / Mozilla Firefox Download Dialog Source Spoofing (Updated)**
  - **Mozilla / Firefox Download Spoofing Vulnerability (Updated)**
  - **Mozilla Firefox Image Javascript URI Dragging Cross-Site Scripting Vulnerability (Updated)**
  - **Multiple Vendor TCP Sequence Number Approximation (Updated)**
  - **Multiple Vendors OpenPGP CFB Mode Vulnerable to Cipher-Text Attack (Updated)**
  - Nokia Symbian OS Phone Denial of Service Vulnerability
  - Oracle Database Server UTL_FILE Error Discloses Files to Remote Authenticated Users
  - PHP Arena paBox Cross-Site Scripting vulnerability
  - **PHP Gift Registry Parameter Input Validation (Updated)**
  - **PHP cURL Open_Basedir Restriction Bypass (Updated)**
  - **PHP Multiple Remote Vulnerabilities (Updated)**
  - phpBB 'viewtopic.php' Information Disclosure
  - **phpBB "autologinid" Security Bypass (Updated)**
  - phpBB Signature Script Insertion Vulnerability
  - phpBB Group phpBB 'oracle.php' Information Disclosure
  - phpBB Group phpBB 'usercp_register.php' Cross-Site Scripting Vulnerability
  - **phpMyAdmin Cross-Site Scripting and Information Disclosure Vulnerabilities (Updated)**
  - phpMyFaq SQL Injection Vulnerability
  - PHPNews 'auth.php' Flaw Permits Remote Code Execution
  - PhpOutsourcing Zorum Cross-Site Scripting Vulnerability
  - PixelApes SafeHTML Remote Code Execution Vulnerability
  - RealNetworks RealPlayer SMIL Error Permits Remote Code Execution
  - RealNetworks RealPlayer WAV File Error Permits Remote Code Execution
  - Smarter Scripts The Includer Remote Code Execution Vulnerability
  - **Squid Error in Parsing HTTP Headers (Updated)**
  - Stadtaus Download Center Lite Arbitrary File Inclusion Vulnerability
  - Stadtaus Tell a Friend Script Remote Code Execution Vulnerability
  - Stadtaus Form Mail Script Lets Remote Users Include and Execute Arbitrary PHP Code
  - TYPO3 SQL Injection Vulnerability
  - Woltlab Burning Board Input Validation Vulnerabilities

Bugs, Holes, & Patches

The table below summarizes vulnerabilities that have been identified, even if they are not being exploited. Complete details about patches or workarounds are available from the source of the information or from the URL provided in the section. CVE numbers are listed where applicable. Vulnerabilities that affect **both** Windows and Unix Operating Systems are included in the Multiple Operating Systems section.

Note: All the information included in the following tables has been discussed in newsgroups and on web sites.

The Risk levels defined below are based on how the system may be impacted:

- **High** - A high-risk vulnerability is defined as one that will allow an intruder to immediately gain privileged access (e.g., sysadmin or root) to the system or allow an intruder to execute code or alter arbitrary system files. An example of a high-risk vulnerability is one that allows an unauthorized user to send a sequence of instructions to a machine and the machine responds with a command prompt with administrator privileges.
- **Medium** - A medium-risk vulnerability is defined as one that will allow an intruder immediate access to a system with less than privileged access. Such vulnerability will allow the intruder the opportunity to continue the attempt to gain privileged access. An example of medium-risk vulnerability is a server configuration error that allows an intruder to capture the password file.
- **Low** - A low-risk vulnerability is defined as one that will provide information to an intruder that could lead to further compromise attempts or a Denial of Service (DoS) attack. It should be noted that while the DoS attack is deemed low from a threat potential, the frequency of this type of attack is very high. DoS attacks against mission-critical nodes are not included in this rating and any attack of this nature should instead be considered to be a "High" threat.

Windows Operating Systems Only

Vendor & Software Name	Vulnerability - Impact Patches - Workarounds Attacks Scripts	Common Name / CVE Reference	Risk	Source
ArGo Software Design FTP Server 1.4.2 .8	A buffer overflow vulnerability exists in the 'DELE' command, which could let a remote malicious user cause a Denial of Service or execute arbitrary code. No workaround or patch available at time of publishing. A Proof of Concept exploit has been published.	ArGoSoft FTP Server 'DELE' Command Remote Buffer Overflow CAN-2005-0696	Low/ High (High if arbitrary code can be executed)	Security Focus, 12755, March 8, 2005
Cerulean Studios Trillian 3.0, Trillian Pro 3.0	A buffer overflow vulnerability exists due to insecure image data copying into finite process buffers, which could let a remote malicious user execute arbitrary code. Cerulean Studios has released an upgrade dealing with this issue. Please contact the vendor for more information on obtaining updated packages. An exploit script has been published.	Cerulean Studios Trillian Insecure Image Data Remote Buffer Overflow CAN-2005-0633	High	Security Focus, 12703, March 2, 2005
Computalynx Limited CProxy Server 3.3 SP2, 3.4.1, 3.4.3, 3.4.4	Several vulnerabilities exist: a Directory Traversal vulnerability exits due to insufficient sanitization of user-supplied input, which could let a remote malicious user obtain sensitive information; and a remote Denial of Service vulnerability exists when a malicious user submits an HTTP GET request to retrieve an ASCII file or an HTTP request to retrieve an executable file. No workaround or patch available at time of publishing. There is no exploit code required; however, a Proof of Concept exploit has been published.	Computalynx CProxy Directory Traversal & Remote Denial of Service CAN-2005-0657	Low/ Medium (Medium if sensitive information can be obtained)	Security Tracker Alert, 1013359, March 2, 2005
Computer Associates Unicenter Asset Management 4.0	Multiple vulnerabilities exist: a vulnerability exists in the admin console in the 'Change Credentials for Database' window because it is possible to obtain the Admin password, an input validation vulnerability exists in the Reporter, which could let a remote malicious user execute arbitrary HTML and script code; and an input validation vulnerability exists in Query Designer when importing queries, which could let a remote malicious user inject arbitrary SQL code in an imported files. Update available at:	Computer Associates Unicenter Asset Management Multiple Vulnerabilities CAN-2005-0640 CAN-2005-0641	Medium/ High (High if arbitrary code can be executed)	Secunia Advisory, SA14454, March 2, 2005

	http://supportconnect.ca.com/sc/solcenter/ solresults.jsp?aparno=Qo64323 There is no exploit code required.	CAN-2005-0642		
Gene6 G6 FTP Server 2.0, 3.0-3.0.2, 3.1, 3.2, 3.3, 3.3.1, 3.4	A vulnerability exists due to a failure to secure critical functionality from default users, which could let a remote malicious user execute arbitrary code with SYSTEM privileges. Workaround: - create a new administrator account - in Administration / Properties, uncheck Options / Allow all access to localhost. Do not forget to adjust the "local machine" properties to use the new administration account. There is no exploit code required; however, a Proof of Concept exploit has been published.	Gene6 FTP Server Insecure Critical Functionality CAN-2005-0690	High	Security Focus, 12739, March 7, 2005
Hosting Controller Hosting Controller 1.1, 1.3, 1.4 b, 1.4, 1.4.1, 6.1 Hotfix 1.7, 6.1 Hotfix 1.4, 6.1	Two vulnerabilities exist: a vulnerability exists because the site updates log is inside the web root, which could let a remote malicious user obtain sensitive information; and a vulnerability exists in the admin login page due to an error in the password recovery feature, which could let a remote malicious user obtain sensitive information. *Note: Successful exploitation requires that the owner's domain name is known.* No workaround or patch available at time of publishing. There is no exploit code required; however, a Proof of Concept exploit has been published.	Hosting Controller Multiple Information Disclosure CAN-2005-0694 CAN-2005-0695	Medium	Secunia Advisory, SA14522, March 8, 2005
JoWood Productions Chaser 1.0, 1.50	A buffer overflow vulnerability exists due to insecure copying of user-supplied input into finite process buffers, which could let a remote malicious user cause a Denial of Service or execute arbitrary code. No workaround or patch available at time of publishing. An exploit script has been published.	JoWood Chaser Remote Buffer Overflow CAN-2005-0693	Low/High (High if arbitrary code can be executed)	Security Focus, 12733, March 7, 2005
KMiNT21 Software Golden FTP Server 1.0 0b, 1.20 b, 1.30 b, 1.31 b, 1.92	A buffer overflow vulnerability exists in the 'USER' command due to insufficient bounds checking, which could let a remote malicious user execute arbitrary code. No workaround or patch available at time of publishing. A Proof of Concept exploit script has been published.	Golden FTP Server 'USER" Remote Buffer Overflow CAN-2005-0634	High	Security Focus, 12704, March 2, 2005
Microsoft Office XP SP2 & SP3, Project 2002, Visio 2002, Works Suite 2002, 2003, 2004	A buffer overflow vulnerability exists due to a boundary error in the process that passes URL file locations to Office, which could let a remote malicious user execute arbitrary code. Patches available at: http://www.microsoft.com/technet/ security/bulletin/MS05-005.mspx V1.1: Bulletin updated to clarify prerequisites under Visio 2002 Update Information. V1.2: Bulletin updated to add an additional FAQ as well as clarify install steps under Update Information. **V1.3: Bulletin updated to add a feature list for all products under the Update Information section, Administrative Installation details.** Currently we are not aware of any exploits for this vulnerability.	Microsoft Office URL File Location Handling Buffer Overflow CAN-2004-0848	High	Microsoft Security Bulletin, MS05-005, February 8, 2005 US-CERT Technical Cyber Security Alert TA05-039A US-CERT Cyber Security Alert SA05-039A US-CERT VU#416001 Microsoft Security Bulletin, MS05-005 V1.1, February 15, 2005 Microsoft Security Bulletin,

	MS05-005 V1.2, February 23, 2005 **Microsoft Security Bulletin, MS05-005 V1.3, March 3, 2005**

Microsoft Windows (XP SP2 is not affected)	A Denial of Service vulnerability exists in the parsing of ANI files. A remote user can cause the target user's system to hang or crash. A remote user can create a specially crafted Windows animated cursor file (ANI file) that, when loaded by the target user, will cause the target system to crash. The malicious file can be loaded via HTML, for example. Updates available at: http://www.microsoft.com/technet/security/bulletin/ms05-002.mspx Bulletin V1.1 (January 20, 2005): Updated CAN reference and added acknowledgment to finder for CAN-2004-1305. **V1.2 Frequently Asked Questions updated to reflect Windows 98, 98SE and ME security update availability.** Another exploit script has been published.	Microsoft Windows ANI File Parsing Errors CAN-2004-1305	Low	VENUSTECH Security Lab, December 23, 2004 Microsoft Security Bulletin MS05-002, January 11, 2005 US-CERT Vulnerability Notes, VU#177584 & VU#697136, January 11, 2005 Security Focus, January 12, 2005 Technical Cyber Security Alert, TA05-012A, January 12, 2005 Microsoft Security Bulletin, MS05-002, V1.1, January 20, 2005 PacketStorm, January 31, 2005 **Microsoft Security Bulletin, MS05-002, V1.2, March 8, 2005 `**
Microsoft Windows (XP SP2 is not affected)	An integer overflow vulnerability was reported in the LoadImage API. A remote user can execute arbitrary code. A remote user can create a specially crafted image file that, when processed by the target user, will trigger an overflow in the USER32 library LoadImage API and execute arbitrary code. The code will run with the privileges of the target user. Updates available at: http://www.microsoft.com/technet/security/bulletin/ms05-002.mspx **V1.2 Frequently Asked Questions updated to reflect Windows 98, 98SE and ME security update availability.** A Proof of Concept exploit has been published.	Microsoft Windows LoadImage API Buffer Overflow CAN-2004-1049	High	VENUSTECH Security Lab. December 23, 2004 Microsoft Security Bulletin MS05-002, January 11, 2005 US-CERT Vulnerability Note, VU#625856, January 11, 2005 Technical Cyber Security Alert, TA05-012A, January 12,

				2005 **Microsoft Security Bulletin, MS05-002, V1.2, March 8, 2005**
Microsoft Windows 2000 SP3 & SP4, Windows XP SP1 & SP2, Windows XP 64-Bit Edition SP1, (Itanium), Windows XP 64-Bit Edition Version 2003 (Itanium), Windows Server 2003, Windows Server 2003 for Itanium-based Systems	A buffer overflow vulnerability exists in the Hyperlink Object Library when handling hyperlinks, which could let a remote malicious user execute arbitrary code. Patches available at: http://www.microsoft.com/technet/security/bulletin/MS05-015.mspx V1.1: Mitigating factor for ISA 2004 updated. **V1.2: Frequently Asked Questions updated to reflect Windows 98, 98SE and ME security update availability.** Currently we are not aware of any exploits for this vulnerability.	Microsoft Windows Hyperlink Object Library Buffer Overflow CAN-2005-0057	High	Microsoft Security Bulletin, MS05-015, February 8, 2005 US-CERT Technical Cyber Security Alert TA05-039A US-CERT Cyber Security Alert SA05-039A US-CERT Vulnerability Note VU#820427 Microsoft Security Bulletin, MS05-015 V1.1, February 15, 2005 **Microsoft Security Bulletin, MS05-015 V1.2, March 8, 2005**
Microsoft Windows Server 2003 Datacenter Edition, Enterprise Edition, Standard Edition, Web Edition, Windows XP Home Edition, XP Professional	A remote Denial of Service vulnerability exists due to improper handling of IP packets that contain the same destination and source IP and the SYN flag set. No workaround or patch available at time of publishing. An exploit script has been published.	Microsoft Windows LAND Attack Remote Denial of Service CAN-2005-0688	Low	Secunia Advisory, A14512, March 7, 2005

SafeNet Sentinel License Manager 7.2.0.2	A buffer overflow vulnerability exists in the 'Lservnt' service on UDP port 5093 due to a boundary error, which could let a remote malicious user execute arbitrary code with SYSTEM privileges. Upgrade to version 8.0 Currently we are not aware of any exploits for this vulnerability.	SafeNet Sentinel License Manager Remote Buffer Overflow CAN-2005-0353	High	CIRT.DK Advisory, March 7, 200 US-CERT VU#108790
TrackerCam TrackerCam 5.12	Multiple vulnerabilities exist: a buffer overflow vulnerability exists in the TrackerCam HTTP server, which could let a remote malicious user execute arbitrary code; a buffer overflow vulnerability exists in TrackerCam PHP scripts due to insufficient bounds checks on arguments, which could let a remote malicious user execute arbitrary code; a Directory Traversal vulnerability exists in the 'ComGetLogFile.php3' script, which could let a remote malicious user obtain sensitive information; a vulnerability exists due to insufficient sanitization of HTML content in the username and password fields, which could let a remote malicious user launch phishing style attacks; and multiple remote Denial of Service vulnerabilities exist. No workaround or patch available at time of publishing. **An exploit script has been published.**	TrackerCam Multiple Remote Vulnerabilities CAN-2005-0478 CAN-2005-0479 CAN-2005-0480 CAN-2005-0481 CAN-2005-0482	Low/ Medium/ High (Low of a DoS; medium if sensitive information can be obtained; and High if arbitrary code can be executed)	Security Focus, 12592, February 18, 2005 **Security Focus, 12592, March 3, 2005**

[back to top]

UNIX / Linux Operating Systems Only

Vendor & Software Name	Vulnerability - Impact Patches - Workarounds Attacks Scripts	Common Name / CVE Reference	Risk	Source
Abuse Abuse 2.0	Multiple vulnerabilities exist in the SDL port, including buffer overflows and an insecure file creation vulnerability, which could let a malicious user execute arbitrary code or overwrite arbitrary files with super user privileges. Debian: http://security.debian.org/pool/updates/main/a/abuse/ Currently we are not aware of any exploits for these vulnerabilities.	Abuse Multiple Vulnerabilities CAN-2005-0098 CAN-2005-0099	High	Debian Security Advisory, D 691-1, March 7, 2005
bidwatcher bidwatcher 1.3-1.3.16	A vulnerability exists due to a failure of the application to properly implement a formatted string function, which could let a remote malicious user execute arbitrary code. Upgrades available at: http://prdownloads.sourceforge.net/ bidwatcher/bidwatcher-1.3.17.tar.gz Debian: http://security.debian.org/pool/ updates/main/b/bidwatcher/ **Gentoo:** **http://security.gentoo.org/ glsa/glsa-200503-06.xml** Currently we are not aware of any exploits for this vulnerability.	Bidwatcher Remote Format String CAN-2005-0158	High	Debian Security Advisory DS 687-1, February 18, 2005 **Gentoo Linux Security Advisory, GLSA 200503-06 March 3, 2005**
BrT CopperExport 0.1, 0.2	A vulnerability exists in 'xp_publish.php' due to insufficient sanitization before used in a SQL query, which could let a remote malicious user inject arbitrary SQL code. Upgrades available at: http://download.berlios.de/copperexport/CopperExport-0.2.1.zip There is no exploit code required.	BrT CopperExport 'XP_Publish.PHP' SQL Injection CAN-2005-0697	High	Secunia Advisory, SA14401 March 7, 2005
Carnegie Mellon University Cyrus IMAP Server 2.x	Multiple vulnerabilities exist: a buffer overflow vulnerability exists in mailbox handling due to an off-by-one boundary error, which could let a remote malicious user execute arbitrary code; a buffer overflow vulnerability exists in the imapd annotate extension due to an off-by-one boundary error, which could let a remote malicious user execute arbitrary code; a buffer overflow vulnerability exists in 'fetchnews,' which could let a remote malicious user execute arbitrary code; a buffer overflow vulnerability exist because remote administrative users can exploit the backend; and a buffer overflow vulnerability exists in imapd due to a boundary error, which could let a remote malicious user execute arbitrary code. Update available at: http://ftp.andrew.cmu.edu/pub/cyrus/ cyrus-imapd-2.2.11.tar.gz Gentoo: http://security.gentoo.org/ glsa/glsa-200502-29.xml	Cyrus IMAP Server Multiple Remote Buffer Overflows CAN-2005-0546	High	Secunia Advisory, SA14383, February 24, 200 Gentoo Linux Security Advisory, GLSA 200502-29, February 23, 2005 SUSE Security Announceme SUSE-SA:2005:009, Februa 24, 2005 Ubuntu Security Notice USN-87-1, February 28, 200 **Mandrakelinux Security Update Advisory, MDKSA-2005:051, March 4 2005**

	SUSE: ftp://ftp.SUSE.com/pub/SUSE Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/c/cyrus21-imapd/ **Mandrake:** **http://www.mandrakesecure.net/en/ftp.php** Currently we are not aware of any exploits for these vulnerabilities.			
Carnegie Mellon University Cyrus SASL 1.5.24, 1.5.27, 1.5.28, 2.1.9-2.1.18	Several vulnerabilities exist: a buffer overflow vulnerability exists in 'digestmda5.c,' which could let a remote malicious user execute arbitrary code; and an input validation vulnerability exists in the 'SASL_PATH' environment variable, which could let a malicious user execute arbitrary code. Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/2/ Gentoo: http://security.gentoo.org/glsa/glsa-200410-05.xml Mandrake: http://www.mandrakesecure.net/en/ftp.php RedHat: http://rhn.redhat.com/errata/RHSA-2004-546.html Trustix: ftp://ftp.trustix.org/pub/trustix/updates/ Debian: http://security.debian.org/pool/updates/main/c/cyrus-sasl/ Conectiva: ftp://atualizacoes.conectiva.com.br/ OpenPGK: ftp ftp.openpkg.org FedoraLegacy: http://download.fedoralegacy.org/redhat/ **SUSE:** **ftp://ftp.SUSE.com/pub/SUSE** Currently we are not aware of any exploits for these vulnerabilities.	Cyrus SASL Buffer Overflow & Input Validation CAN-2004-0884 CAN-2005-0373	High	Security Tracker Alert ID: 1011568, October 7, 2004 Debian Security Advisories DSA 563-2, 563-3, & 568-1, October 12, 14, & 16, 2004 Conectiva Linux Security Announcement, CLA-2004:8 November 11, 2004 OpenPKG Security Advisory OpenPKG Security Advisory January 28, 2005 Fedora Legacy Update Advisory, FLSA:2137, Febru 17, 2005 SUSE Security Summary Report, SUSE-SR:2005:006 February 25, 2005 **SUSE Security Announcement, SUSE-SA:2005:013, March 2005**
FreeBSD FreeBSD 5.0 -RELENG, 5.0 -RELEASE-p14, 5.0, 5.1 -RELENG, 5.1 -RELEASE, 5.1, 5.2 -RELENG, 5.2 -RELEASE, 5.2, 5.2.1, 5.3 -STABLE, 5.3 -RELEASE, 5.3	A vulnerability exists related to SMP (Symmetric Multiprocessing), which could let a malicious user obtain sensitive information. No workaround or patch available at time of publishing. Currently we are not aware of any exploits for this vulnerability.	FreeBSD SMP Information Disclosure CAN-2005-0109	Medium	Security Focus, 12724, Marc 4, 2005
gFTP gFTP 0.1, 0.2, 0.21, 1.0, 1.1-1.13, 2.0-2.0.17	A Directory Traversal vulnerability exists due to insufficient sanitization of input, which could let a remote malicious user obtain sensitive information. Upgrades available at: http://www.gftp.org/gftp-2.0.18.tar.gz Debian: http://security.debian.org/pool/updates/main/g/gftp/ Gentoo: http://security.gentoo.org/glsa/glsa-200502-27.xml SUSE: ftp://ftp.SUSE.com/pub/SUSE **Mandrake:** **http://www.mandrakesecure.net/en/ftp.php** There is no exploit code required.	gFTP Remote Directory Traversal CAN-2005-0372	Medium	Security Focus, February 14 2005 Debian Security Advisory, D 686-1, February 17, 2005 SUSE Security Summary Report, SUSE-SR:2005:005 February 18, 2005 Gentoo Linux Security Advisory, GLSA 200502-27, February 19, 2005 **Mandrakelinux Security Update Advisory, MDKSA-2005:050, March 4 2005**

Glyph and Cog XPDF prior to 3.00pl3	A buffer overflow vulnerability exists in ' 'xpdf/Decrypt.cc' due to a boundary error in the 'Decrypt::makeFileKey2' function, which could let a remote malicious user execute arbitrary code. Update available at: http://www.foolabs.com/xpdf/download.html Patch available at: ftp://ftp.foolabs.com/pub/xpdf/xpdf-3.00pl3.patch Debian: http://security.debian.org/pool/updates/main/c/cupsys/ http://security.debian.org/pool/updates/main/x/xpdf/ Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates Gentoo: http://security.gentoo.org/glsa/ KDE: ftp://ftp.kde.org/pub/kde/security_patches Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/ Conectiva: ftp://atualizacoes.conectiva.com.br/ Mandrake: http://www.mandrakesecure.net/en/ftp.php SUSE: ftp://ftp.suse.com/pub/suse/ FedoraLegacy: http://download.fedoralegacy.org/fedora/1/updates/ Gentoo: http://security.gentoo.org/glsa/glsa-200502-10.xml SGI: ftp://patches.sgi.com/support/free/security/advisories/ Trustix: http://http.trustix.org/pub/trustix/updates/ **FedoraLegacy:** **http://download.fedoralegacy.org/redhat/** Currently we are not aware of any exploits for this vulnerability.	Glyph and Cog Xpdf 'makeFileKey2()' Buffer Overflow CAN-2005-0064	High	iDEFENSE Security Advisor January 18, 2005 Conectiva Linux Security Announcement, CLA-2005:9 January 25, 2005 Mandrakelinux Security Upd Advisories, MDKSA-2005:016-021, Janu 26, 2005 SUSE Security Summary Report, SUSE-SR:2005:002 January 26, 2005 SUSE Security Summary Report, SUSE-SR:2005:003 February 4, 2005 SGI Security Advisory, 20050202-01-U, February 9 2005 Gentoo Linux Security Advisory, GLSA 200502-10, February 9, 2005 Fedora Legacy Update Advisory, FLSA:2353, Febru 10, 2005 Trustix Secure Linux Securit Advisory, TSLSA-2005-0003 February 11, 2005 **Fedora Legacy Update Advisory, FLSA:2127, Mar 2, 2005**
GNU Midnight Commander Project Midnight Commander 4.x	Multiple vulnerabilities exist due to various design and boundary condition errors, which could let a remote malicious user cause a Denial of Service, obtain elevated privileges, or execute arbitrary code. Debian: http://security.debian.org/pool/updates/main/m/mc/ SUSE: ftp://ftp.suse.com/pub/suse/ Gentoo: http://security.gentoo.org/glsa/glsa-200502-24.xml **RedHat:** **http://rhn.redhat.com/errata/RHSA-2005-217.html** Currently we are not aware of any exploits for these vulnerabilities.	Midnight Commander Multiple Vulnerabilities CAN-2004-1004 CAN-2004-1005 CAN-2004-1009 CAN-2004-1090 CAN-2004-1091 CAN-2004-1092 CAN-2004-1093 CAN-2004-1174 CAN-2004-1175 CAN-2004-1176	Low/ Medium/ High (Low if a DoS; Medium is elevated privileges can be obtained; and High if arbitrary code can be executed)	Security Tracker Alert, 1012903, January 14, 2005 SUSE Security Summary Report, SUSE-SR:2005:003 February 4, 2005 Gentoo Linux Security Advisory, GLSA 200502-24, February 17, 2005 **RedHat Security Advisory, RHSA-2005:217-10, March 2005**
GNU cpio 1.0, 1.1, 1.2	A vulnerability exists in 'cpio/main.c' due to a failure to create files securely, which could let a malicious user obtain sensitive information. Upgrades available at: http://ftp.gnu.org/gnu/cpio/cpio-2.6.tar.gz **SGI:** **ftp://oss.sgi.com/projects/sgi_**	CPIO Archiver Insecure File Creation CAN-1999-1572	Medium	Security Tracker Alert, 1013041, January 30, 2005 **SGI Security Advisory, 20050204-01-U, March 7, 2**

	[propack/download/3/updates/] There is no exploit required.			
GNU CUPS 1.1.22	A vulnerability was reported in CUPS in the processing of HPGL files. A remote malicious user can cause arbitrary code to be executed by the target user. A remote user can create a specially crafted HPGL file that, when printed by the target user with CUPS, will execute arbitrary code on the target user's system. The code will run with the privileges of the 'lp' user. The buffer overflow resides in the ParseCommand() function in 'hpgl-input.c.' Fixes are available in the CVS repository and are included in version 1.1.23rc1. Fedora: http://download.fedora.redhat.com/pub/ fedora/linux/core/updates/ Mandrake: http://www.mandrakesecure.net/en/ftp.php SGI: http://www.sgi.com/support/security/ SuSE: ftp://ftp.suse.com/pub/suse/ TurboLinux: ftp://ftp.turbolinux.co.jp/pub/ TurboLinux/TurboLinux/ia32/ **FedoraLegacy:** **http://download.fedoralegacy. org/redhat/** A Proof of Concept exploit script has been published.	GNU CUPS HPGL ParseCommand() Buffer Overflow CAN-2004-1267	High	CUPS Advisory STR #1023, December 16, 2004 Mandrakelinux Security Upd Advisory, MDKSA-2005:008 January 17, 2005 SGI Security Advisory, 20050101-01-U, January 19 2005 SUSE Security Summary Report, SUSE-SR:2005:003 February 4, 2005 Turbolinux Security Announcement, February 17 2005 **Fedora Legacy Update Advisory, FLSA:2127, Mar 2, 2005**
GNU CUPS lppasswd 1.1.22	A vulnerability was reported in the CUPS lppasswd utility. A local malicious user can truncate or modify certain files and cause Denial of Service conditions on the target system. There are flaws in the way that lppasswd edits the '/usr/local/etc/cups/passwd' file. Fixes are available in the CVS repository and are included in version 1.1.23rc1. Fedora: http://download.fedora.redhat.com/pub /fedora/linux/core/updates/ RedHat: http://rhn.redhat.com/errata/ RHSA-2005-013.html Mandrake: http://www.mandrakesecure.net/ en/ftp.php SGI: http://www.sgi.com/support/security/ TurboLinux: ftp://ftp.turbolinux.co.jp/pub/ TurboLinux/TurboLinux/ **FedoraLegacy:** **http://download.fedoralegacy. org/redhat/** A Proof of Concept exploit has been published.	GNU CUPS lppasswd Denial of Service CAN-2004-1268	Low	Security Tracker Alert ID, 1012602, December 16, 200 Mandrakelinux Security Upd Advisory, MDKSA-2005:008 January 17, 2005 SGI Security Advisory, 20050101-01-U, January 19 2005 Turbolinux Security Announcement, February 17 2005 **Fedora Legacy Update Advisory, FLSA:2127, Mar 2, 2005**
GNU Xpdf prior to 3.00pl2	A buffer overflow vulnerability exists that could allow a remote user to execute arbitrary code on the target user's system. A remote user can create a specially crafted PDF file that, when viewed by the target user, will trigger an overflow and execute arbitrary code with the privileges of the target user. A fixed version (3.00pl2) is available at: http://www.foolabs.com/xpdf/download.html A patch is available: ftp://ftp.foolabs.com/pub/xpdf/ xpdf-3.00pl2.patch KDE: http://www.kde.org/info/security/ advisory-20041223-1.txt Gentoo: http://security.gentoo.org/glsa /glsa-200412-24.xml Fedora:	GNU Xpdf Buffer Overflow in doImage() CAN-2004-1125	High	iDEFENSE Security Advisor 12.21.04 KDE Security Advisory, December 23, 2004 Mandrakesoft, MDKSA-2004:161,162,163, 166, December 29, 2004 Fedora Update Notification, FEDORA-2004-585, Januar 2005 Gentoo Linux Security Advisory, GLSA 200501-13, January 10, 2005 Conectiva Linux Security Announcement, CLA-2005:9 January 25, 2005

	http://download.fedora.redhat.com/pub/fedora/linux/core/updates/ Ubuntu: http://security.ubuntu.com/ubuntu/pool/ Mandrakesoft (update for koffice): http://www.mandrakesoft.com/security/advisories?name=MDKSA-2004:165 Mandrakesoft (update for kdegraphics): http://www.mandrakesoft.com/security/advisories?name=MDKSA-2004:163 Mandrakesoft (update for gpdf): http://www.mandrakesoft.com/security/advisories?name=MDKSA-2004:162 Mandrakesoft (update for xpdf): http://www.mandrakesoft.com/security/advisories?name=MDKSA-2004:161 Mandrakesoft (update for tetex): http://www.mandrakesoft.com/security/advisories?name=MDKSA-2004:166 Debian: http://www.debian.org/security/2004/dsa-619 Fedora (update for tetex): http://download.fedora.redhat.com/pub/fedora/linux/core/updates/ Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/3/ Gentoo: http://security.gentoo.org/glsa/glsa-200501-13.xml TurboLinux: ftp://ftp.turbolinux.co.jp/pub/TurboLinux/TurboLinux/ia32/ SGI: http://support.sgi.com/browse_request/linux_patches_by_os Conectiva: ftp://atualizacoes.conectiva.com.br/ SuSE: ftp://ftp.suse.com/pub/suse/ FedoraLegacy: http://download.fedoralegacy.org/fedora/1/updates/ **FedoraLegacy: http://download.fedoralegacy.org/redhat/** Currently we are not aware of any exploits for this vulnerability.			SUSE Security Summary Report, SUSE-SR:2005:002 January 26, 2005 Avaya Security Advisory, ASA-2005-027, January 25, 2005 SUSE Security Summary Report, SUSE-SR:2005:003 February 4, 2005 SUSE Security Summary Report, SUSE-SR:2005:003 February 4, 2005 Fedora Legacy Update Advisory, FLSA:2353, Febru 10, 2005 **Fedora Legacy Update Advisory, FLSA:2127, Mar 2, 2005**
Hashcash Hashcash 1.0-1.16	A format string vulnerability exists due to the way the 'From:' mail header is handled, which could let a remote malicious user execute arbitrary code. Gentoo: http://security.gentoo.org/glsa/glsa-200503-12.xml Currently we are not aware of any exploits for this vulnerability.	Hashcash 'From:' Email Reply Header Format String CAN-2005-0687	High	Gentoo Linux Security Advisory, GLSA 200503-12, March 7, 2005
Hewlett Packard Company HP-UX B.11.23, HP-UX B.11.11, HP-UX B.11.00	A remote Denial of Service vulnerability exists due to a failure to handle malformed network data. Upgrades available at: http://software.hp.com/ Currently we are not aware of any exploits for this vulnerability.	HP-UX BIND Remote Denial of Service CAN-2005-0364	Low	HP Security Bulletin, HPSBUX01117, February 9 2005 **HP Security Bulletin, HPSBUX01117, Revision 1 March 2, 2005**
Hiroyuki Yamamoto Sylpheed 0.8.11, 0.9.4-0.9.12, 0.9.99, 1.0 .0-1.0.2	A buffer overflow vulnerability exists in certain headers that contain non-ASCII characters, which could let a remote malicious user execute arbitrary code. Upgrades available at: http://sylpheed.good-day.net/sylpheed/v1.0/sylpheed-1.0.3.tar.gz Currently we are not aware of any exploits for this vulnerability.	Sylpheed Mail Client Remote Buffer Overflow CAN-2005-0667	High	Security Tracker Alert, 1013376, March 4, 2005

John Bradley XV 3.10 a	A format string vulnerability exists in a formatted printing function due to insufficient sanitization of user-supplied input, which could let a remote malicious user cause a Denial of Service or execute arbitrary code. Gentoo: http://security.gentoo.org/glsa/glsa-200503-09.xml Currently we are not aware of any exploits for this vulnerability.	XV File Name Handling Remote Format String CAN-2005-0665	Low/ High (High if arbitrary code can be executed)	Gentoo Linux Security Advisory, GLSA 200503-09, March 4, 2005
KDE kdelibs 3.3.2	A vulnerability exists in the 'dcopidling' library due to insufficient validation of a files existence, which could let a malicious user corrupt arbitrary files. Patch available at: http://bugs.kde.org/attachment.cgi?id=9205&action=view Mandrake: http://www.mandrakesecure.net/en/ftp.php **Gentoo:** **http://security.gentoo.org/glsa/glsa-200503-14.xml** Currently we are not aware of any exploits for this vulnerability.	KDE 'DCOPIDLING' Library CAN-2005-0365	Medium	Security Focus, February 11 2005 **Mandrakelinux** Security Update Advisory, MDKSA-2005:045, February 18, 2005 **Gentoo Linux Security Advisory, GLSA 200503-14 March 7, 2005**
libexif libexif 0.6.9, 0.6.11	A vulnerability exists in the 'EXIF' library due to insufficient validation of 'EXIF' tag structure, which could let a remote malicious user execute arbitrary code. Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/libe/libexif/ Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/ Currently we are not aware of any exploits for this vulnerability.	LibEXIF Library EXIF Tag Structure Validation CAN-2005-0664	High	Ubuntu Security Notice USN-91-1, March 7, 2005 Fedora Update Notifications FEDORA-2005-199 & 200, March 8, 2005
libtiff.org LibTIFF 3.6.1 Avaya MN100 (All versions), Avaya Intuity LX (version 1.1-5.x), Avaya Modular Messaging MSS (All versions)	Several buffer overflow vulnerabilities exist: a vulnerability exists because a specially crafted image file can be created, which could let a remote malicious user cause a Denial of Service or execute arbitrary code; a remote Denial of Service vulnerability exists in 'libtiff/tif_dirread.c' due to a division by zero error; and a vulnerability exists in the 'tif_next.c,' 'tif_thunder.c,' and 'tif_luv.c' RLE decoding routines, which could let a remote malicious user execute arbitrary code. Debian: http://security.debian.org/pool/updates/main/t/tiff/ Gentoo: http://security.gentoo.org/glsa/glsa-200410-11.xml Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/2/ OpenPKG: ftp://ftp.openpkg.org/release/ Trustix: ftp://ftp.trustix.org/pub/trustix/updates/ Mandrake: http://www.mandrakesecure.net/en/ftp.php SuSE: ftp://ftp.suse.com/pub/suse/ RedHat: http://rhn.redhat.com/errata/RHSA-2004-577.html Slackware: ftp://ftp.slackware.com/pub/slackware/ Conectiva: ftp://atualizacoes.conectiva.com.br/ KDE: Update to version 3.3.2: http://kde.org/download/ Apple Mac OS X: http://www.apple.com/swupdates/ Gentoo: KDE kfax: http://www.gentoo.org/security	LibTIFF Buffer Overflows CAN-2004-0803 CAN-2004-0804 CAN-2004-0886	Low/High (High if arbitrary code can be execute)	Gentoo Linux Security Advisory, GLSA 200410-11, October 13, 2004 Fedora Update Notification, FEDORA-2004-334, Octobe 14, 2004 OpenPKG Security Advisory OpenPKG-SA-2004.043, October 14, 2004 Debian Security Advisory, D 567-1, October 15, 2004 Trustix Secure Linux Securit Advisory, TSLSA-2004-0054 October 15, 2004 Mandrakelinux Security Upd Advisory, MDKSA-2004:109 MDKSA-2004:111, October & 21, 2004 SuSE Security Announceme SUSE-SA:2004:038, Octobe 22, 2004 RedHat Security Advisory, RHSA-2004:577-16, Octobe 22, 2004 Slackware Security Advisory SSA:2004-305-02, Novembe 1, 2004 Conectiva Linux Security Announcement, CLA-2004:8 November 8, 2004 US-CERT Vulnerability Note VU#687568 & VU#948752, December 1, 2004 Gentoo Linux Security Advisory, GLSA 200412-02, December 6, 2004 KDE Security Advisory,

	/en/glsa/glsa-200412-17.xml Avaya: No solution but workarounds available at: http://support.avaya.com/elmodocs2/security/ASA-2005-002_RHSA-2004-577.pdf TurboLinux: http://www.turbolinux.com/update/ **Mandrake:** **http://www.mandrakesecure.net/en/ftp.php** Proofs of Concept exploits have been published.			December 9, 2004 Apple Security Update SA-2004-12-02 Gentoo Security Advisory, GLSA 200412-17 / kfax, December 19, 2004 Avaya Advisory ASA-2005-0 January 5, 2005 Conectiva Linux Security Announcement, CLA-2005:9 January 6, 2005 Turbolinux Security Announcement, January 20, 2005 **Mandrakelinux Security Update Advisory, MDKSA-2005:052, March 4 2005**
mlterm mlterm 2.5, 2.6-2.6.3, 2.7, 2.8, 2.9, 2.9.1	An integer overflow vulnerability exists due to insufficient sanity checks of malformed image files, which could let a remote malicious user execute arbitrary code. Upgrades available at: http://prdownloads.sourceforge.net/mlterm/mlterm-2.9.2.tar.gz?download Gentoo: http://security.gentoo.org/glsa/glsa-200503-13.xml Currently we are not aware of any exploits for this vulnerability.	Mlterm Background Image Integer Overflow CAN-2005-0686	High	Gentoo Linux Security Advisory, GLSA 200503-13, March 7, 2005
Multiple Vendors ClamAV 0.51-0.54, 0.60, 0.65, 0.67, 0.68 -1, 0.68, 0.70, 0.80 rc1-rc4, 0.80; MandrakeSoft Corporate Server 3.0 x86_64, 3.0. Linux Mandrake 10.1 X86_64, 10.1	A remote Denial of Service vulnerability exists due to an error in the handling of file information in corrupted ZIP files. Upgrade available at: http://sourceforge.net/project/showfiles.php?group_id=86638&release_id=300116 Gentoo: http://security.gentoo.org/glsa/glsa-200501-46.xml Mandrake: http://www.mandrakesecure.net/en/ftp.php SUSE: ftp://ftp.SUSE.com/pub/SUSE Trustix: http://www.trustix.org/errata/2005/0003/ **Conectiva:** **ftp://atualizacoes.conectiva.com.br/10/RPMS/libclamav-devel-static-0.83-70136U10_7cl.i386.rpm** Currently we are not aware of any exploits for this vulnerability.	Clam Anti-Virus ClamAV Remote Denial of Service CAN-2005-0133	Low	Security Focus, January 31, 2005 Mandrakelinux Security Upd Advisory, MDKSA-2005:025 January 31, 2005 Gentoo Linux Security Advisory, GLSA 200501-46, January 31, 2005 SUSE Security Summary Report, SUSE-SR:2005:003 February 4, 2005 Trustix Secure Linux Securit Advisory, TSLSA-2005-0003 February 11, 2005 **Conectiva Linux Security Announcement, CLA-2005:928, March 3, 20**
Multiple Vendors Linux kernel 2.6.10, 2.6.9; RedHat Fedora Core2&3	A Denial of Service vulnerability exists in the 'mlockall()' system call due to a failure to properly enforce defined limits. Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/ RedHat: https://rhn.redhat.com/errata/RHSA-2005-092.html **Conectiva:** **ftp://atualizacoes.conectiva.com.br/** A Proof of Concept exploit script has been published.	Linux Kernel Local RLIMIT_MEMLOCK Bypass Denial of Service CAN-2005-0179	Low	Bugtraq, January 7, 2005 Fedora Update Notifications FEDORA-2005-013 & 014, January 10, 2005 RedHat Security Advisory, RHSA-2005:092-14, Februa 18, 2005 **Conectiva Linux Security Announcement, CLA-2005:930, March 7, 20**
Multiple Vendors Bernd Johanness Wueb kppp 1.1.3; KDE KDE 1.1-1.1.2, 1.2, 2.0 BETA, 2.0-2.2.2, 3.0-3.0.5, 3.1-3.1.5, KDE KPPP 2.1.2	A vulnerability exists due to a file descriptor leak, which could let a malicious user obtain sensitive information. Patch available at: ftp://ftp.kde.org/pub/kde/security_patches **RedHat:** **http://rhn.redhat.com/errata/RHSA-2005-175.html**	KPPP Privileged File Descriptor Information Disclosure CAN-2005-0205	Medium	iDEFENSE Security Advisor February 28, 2005 **RedHat Security Advisory, RHSA-2005:175-06, March 2005** **Debian Security Advisory, DSA 692-1, March 8, 2005**

	Debian: **http://security.debian.org/pool/updates/main/k/kdenetwork/** There is no exploit code required.			
Multiple Vendors Gentoo Linux; Samba Samba 3.0-3.0.7	A remote Denial of Service vulnerability exists in 'ms_fnmatch()' function due to insufficient input validation. Patch available at: http://us4.samba.org/samba/ftp/patches/security/samba-3.0.7-CAN-2004-0930.patch Gentoo: http://security.gentoo.org/glsa/glsa-200411-21.xml Mandrake: http://www.mandrakesecure.net/en/ftp.php SuSE: ftp://ftp.suse.com/pub/suse/i386/update/ Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/s/samba/ RedHat: http://rhn.redhat.com/errata/RHSA-2004-632.html Trustix: http://http.trustix.org/pub/trustix/updates/ Conectiva: ftp://atualizacoes.conectiva.com.br/ Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/ SGI: http://www.sgi.com/support/security/ TurboLinux: ftp://ftp.turbolinux.co.jp/pub/TurboLinux/TurboLinux/ia32/Server/10/updates/ OpenPKG: http://www.openpkg.org/security.html **SCO:** **ftp://ftp.sco.com/pub/updates/UnixWare/SCOSA-2005.17** There is no exploit code required.	Multiple Vendors Samba Remote Wild Card Denial of Service CAN-2004-0930	Low	Security Focus, November 1 2004 Trustix Secure Linux Securit Advisory, TSLSA-2004-005 November 16, 2004 RedHat Security Advisory, RHSA-2004:632-17, Novem 16, 2004 Conectiva Linux Security Announcement, CLA-2004: November 25, 2004 Fedora Update Notifications FEDORA-2004-459 & 460, November 29, 2004 Turbolinux Security Advisor TLSA-2004-32, December 2004 SGI Security Advisory, 20041201-01-P, December 2004 OpenPKG Security Advisory OpenPKG-SA-2004.054 December 17, 2004 **SCO Security Advisory, SCOSA-2005.17, March 7, 2005**
Multiple Vendors ImageMagick 5.3.3, 5.4.3, 5.4.4 .5, 5.4.7, 5.4.8 .2-1.1.0, 5.4.8, 5.5.3 .2-1.2.0, 5.5.6 .0-20030409, 5.5.7, 6.0-6.0.8, 6.1-6.1.7, 6.2	A format string vulnerability exists when handling malformed file names, which could let a remote malicious user cause a Denial of Service or execute arbitrary code. Update available at: http://www.imagemagick.org/script/downloads.php Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/i/imagemagick/ Currently we are not aware of any exploits for this vulnerability.	ImageMagick File Name Handling Remote Format String CAN-2005-0397	Low/ High (High if arbitrary code can be executed)	Secunia Advisory, SA14466, March 4, 2005 Ubuntu Security Notice, USN-90-1, March 3, 2004
Multiple Vendors Linux Kernel 2.4 - 2.4.28, 2.6 - 2.6.9; Avaya Intuity LX, Avaya MN100, Avaya Modular Messaging (MSS) 1.1, 2.0	Several vulnerabilities exist in the Linux kernel in the processing of IGMP messages. A local user may be able to gain elevated privileges. A remote user can cause the target system to crash. These are due to flaws in the ip_mc_source() and igmp_marksources() functions. SUSE: http://www.novell.com/linux/security/advisories/2004_44_kernel.html Trustix: http://http.trustix.org/pub/trustix/updates/ Ubuntu: http://security.ubuntu.com/ubuntu/pool Fedora:	Multiple Vendors Linux Kernel IGMP Integer Underflow CAN-2004-1137	Low/ Medium (Medium if elevated privileges can be obtained)	iSEC Security Research Advisory 0018, December 1 2004 Security Focus, December 2005 Secunia, SA13706, January 2005 Avaya Security Advisory, ASA-2005-006, January 14, 2006 Mandrake Security Advisory MDKSA-2005:022, January

	http://download.fedora.redhat.com/pub/fedora/linux/core/updates/ Avaya: http://support.avaya.com/elmodocs2/security/ASA-2005-006_RHSA-2004-549 RHSA-2004-505RHSA-2004-689.pdf Mandrake: http://www.mandrakesecure.net/en/ftp.php RedHat: https://rhn.redhat.com/errata/RHSA-2005-092.html TurboLinux: ftp://ftp.turbolinux.co.jp/pub/TurboLinux/TurboLinux/ FedoraLegacy: http://download.fedoralegacy.org/redhat/ **Conectiva:** **ftp://atualizacoes.conectiva.com.br/** A Proof of Concept exploit script has been published.			2005 RedHat Security Advisory, RHSA-2005:092-14, Februa 18, 2005 Turbolinux Security Announcement , February 2 2005 Fedora Legacy Update Advisory, FLSA:2336, Febru 24, 2005 **Conectiva Linux Security Announcement, CLA-2005:930, March 7, 20**
Multiple Vendors Linux Security Modules (LSM); Ubuntu Linux 4.1 ppc, ia64, ia32	A security issue in Linux Security Modules (LSM) may grant normal user processes escalated privileges. When loading the Capability LSM module as a loadable kernel module, all existing processes gain unintended capabilities granting them root privileges. Only use the Capability LSM module when compiled into the kernel and grant only trusted users access to affected systems. Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.8.1/ **Conectiva:** **ftp://atualizacoes.conectiva.com.br/** Currently we are not aware of any exploits for this vulnerability.	Multiple Vendors Linux Security Modules Escalation Vulnerability CAN-2004-1337	High	Secunia SA13650, Decemb 27, 2004 Ubuntu Security Notice, USN-57-1, January 9, 2005 **Conectiva Linux Security Announcement, CLA-2005:930, March 7, 20**
Multiple Vendors Samba 3.0 - 3.0.7; RedHat Advanced Workstation for the Itanium Processor 2.1, IA64, Desktop 3.0, Enterprise Linux WS 3, WS 2.1 IA64, 2.1, ES 3, 2.1 IA64, 2.1, AS 3, 2.1 IA64, 2.1; Ubuntu Linux 4.1 ppc, ia64, ia32	A buffer overflow vulnerability exists in the 'QFILEPATHINFO' request handler when constructing 'TRANSACT2_QFILEPATHINFO' responses, which could let a remote malicious user execute arbitrary code. Update available at: http://www.samba.org/samba/download/ Mandrake: http://www.mandrakesecure.net/en/ftp.php SuSE: ftp://ftp.suse.com/pub/suse/ Trustix: ftp://ftp.trustix.org/pub/trustix/updates/ Ubuntu: Ubuntu Upgrade samba-doc_ 3.0.7-1ubuntu6.2_all.deb Conectiva: ftp://atualizacoes.conectiva.com.br/ Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/ TurboLinux: ftp://ftp.turbolinux.co.jp/pub/TurboLinux/TurboLinux/ia32/Server/10/updates/ Red Hat: http://rhn.redhat.com/errata/RHSA-2004-632.html OpenPKG: http://www.openpkg.org/security.html **SCO:** **ftp://ftp.sco.com/pub/updates/UnixWare/SCOSA-2005.17** Currently we are not aware of any exploits for this vulnerability.	Multiple Vendors Samba 'QFILEPATHINFO' Buffer Overflow CAN-2004-0882	High	e-matters GmbH Security Advisory, November 14, 200 SuSE Security Announceme SUSE-SA:2004:040, Novem 15, 2004 Trustix Secure Linux Securit Advisory, TSLSA-2004-0058 November 16, 2004 Ubuntu Security Notice, USN-29-1, November 18, 20 Mandrakelinux Security Upd Advisory, MDKSA-2004:136 November 19, 2004 US-CERT Vulnerability Note VU#457622, November 19, 2004 Conectiva Linux Security Announcement, CLA-2004:8 November 25, 2004 Fedora Update Notifications FEDORA-2004-459 & 460, November 29, 2004 Turbolinux Security Advisory TLSA-2004-32, December 8 2004 Red Hat Security Advisory RHSA-2004:632-17, Novem 16, 2004 OpenPKG Security Advisory OpenPKG-SA-2004.054 December 17, 2004 **SCO Security Advisory, SCOSA-2005.17, March 7,**

				2005
Multiple Vendors Squid Web Proxy Cache 2.0 PATCH2, 2.1 PATCH2, 2.3 .STABLE4&5, 2.4 .STABLE6&7, 2.4 .STABLE2, 2.4, 2.5 .STABLE3-7, 2.5 .STABLE1; Conectiva Linux 9.0, 10.0	Two vulnerabilities exist: remote Denial of Service vulnerability exists in the Web Cache Communication Protocol (WCCP) functionality due to a failure to handle unexpected network data; and buffer overflow vulnerability exists in the 'gopherToHTML()' function due to insufficient validation of user-supplied strings, which could let a remote malicious user execute arbitrary code. Patches available at: http://www.squid-cache.org/Versions/v2/2.5/bugs/squid-2.5.STABLE7-wccp_denial_of_service.patch http://www.squid-cache.org/Versions/v2/2.5/bugs/squid-2.5.STABLE7-gopher_html_parsing.patch Gentoo: http://security.gentoo.org/glsa/glsa-200501-25.xml Debian: http://security.debian.org/pool/updates/main/s/squid/ Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/s/squid/ Mandrake: http://www.mandrakesecure.net/en/ftp.php Conectiva: ftp://atualizacoes.conectiva.com.br/ Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates RedHat: http://rhn.redhat.com/errata/RHSA-2005-061.html SUSE: ftp://ftp.suse.com/pub/suse/ Trustix: http://www.trustix.org/errata/2005/0003/ TurboLinux: ftp://ftp.turbolinux.co.jp/pub/TurboLinux/TurboLinux/ia32/ **Astaro:** **http://www.astaro.org/showflat.php?Cat=&Number=56136&page=0&view=collapsed&sb=5&o=&fpart=1#56136** There is no exploit required.	Squid Proxy Web Cache WCCP Functionality Remote Denial of Service & Buffer Overflow CAN-2005-0094 CAN-2005-0095	Low/High (High if arbitrary code can be executed)	Secunia Advisory, SA13825 January 13, 2005 Debian Security Advisory, D 651-1, January 20, 2005 Ubuntu Security Notice, USN-67-1, January 20, 2005 Mandrakelinux Security Upd Advisory, MDKSA-2005:014 January 25, 2005 Conectiva Linux Security Announcement, CLA-2005:9 January 26, 2005 Fedora Update Notifications FEDORA-2005-105 & 106, February 1, 2005 SUSE Security Summary Report, SUSE-SR:2005:003 February 4, 2005 Trustix Secure Linux Securit Advisory, TSLSA-2005-0003 February 11, 2005 SUSE Security Announceme SUSE-SA:2005:006, Februa 10, 2005 RedHat Security Advisory, RHSA-2005:061-19, Februa 11, 2005 Turbolinux Security Announcement, February 17 2005 **Security Focus, 12275 & 12276, March 7, 2005**
Multiple Vendors Squid Web Proxy Cache 2.5 .STABLE9, .STABLE8, .STABLE7	A vulnerability exists when using the Netscape Set-Cookie recommendations for handling cookies in caches due to a race condition, which could let a malicious user obtain sensitive information. Patches available at: http://www.squid-cache.org/Versions/v2/2.5/bugs/squid-2.5.STABLE9-setcookie.patch Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/s/squid/ There is no exploit code required.	Squid Proxy Set-Cookie Headers Information Disclosure CAN-2005-0626	Medium	Secunia Advisory, SA14451 March 3, 2005 Ubuntu Security Notice, USN-93-1 March 08, 2005

Multiple Vendors Apple Mac OS X 10.2-10.2.8, 10.3 -10.3.5, OS X Server 10.2-10.2.8, 10.3 -10.3.5; Easy Software Products CUPS 1.0.4 -8, 1.0.4, 1.1.1, 1.1.4-5, 1.1.4 -3, 1.1.4 -2, 1.1.4, 1.1.6, 1.1.7, 1.1.10, 1.1.12-1.1.21	A vulnerability exists in 'error_log' when certain methods of remote printing are carried out by an authenticated malicious user, which could disclose user passwords. Update available at: http://www.cups.org/software.php Apple: http://wsidecar.apple.com/cgi-bin/nph-reg3rdpty1.pl/product=04829&platform=osx&method=sa/SecUpd2004-09-30Jag.dmg http://wsidecar.apple.com/cgi-bin/nph-reg3rdpty1.pl/product=04830&platform=osx&method=sa/SecUpd2004-09-30Pan.dmg Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/2/ Gentoo: http://security.gentoo.org/glsa/glsa-200410-06.xml Debian: http://security.debian.org/pool/updates/main/c/cupsys/ Mandrake: http://www.mandrakesecure.net/en/ftp.php RedHat: http://rhn.redhat.com/errata/RHSA-2004-543.html **FedoraLegacy:** **http://download.fedoralegacy.org/redhat/** There is no exploit code required.	CUPS Error_Log Password Disclosure CAN-2004-0923	Medium	Apple Security Update, APPLE-SA-2004-09-30, October 4, 2004 Fedora Update Notification, FEDORA-2004-331, Octobe 2004 Gentoo Linux Security Advisory, GLSA 200410-06, October 9, 2004 Debian Security Advisory, D 566-1, October 14, 2004 Mandrakelinux Security Upd Advisory, MDKSA-2004:116 October 21, 2004 RedHat Security Advisory, RHSA-2004:543-15, Octobe 22, 2004 US-CERT Vulnerability Note VU#557062, November 19, 2004 **Fedora Legacy Update Advisory, FLSA:2127, Mar 2, 2005**
Multiple Vendors Daniel Stenberg curl 6.0-6.4, 6.5-6.5.2, 7.1, 7.1.1, 7.2, 7.2.1, 7.3, 7.4, 7.4.1, 7.10.1, 7.10.3-7.10.7, 7.12.1	A buffer overflow vulnerability exists in the Kerberos authentication code in the 'Curl_krb_kauth()' and 'krb4_auth()' functions and in the NT Lan Manager (NTLM) authentication in the 'Curl_input_ntlm()' function, which could let a remote malicious user execute arbitrary code. SUSE: ftp://ftp.SUSE.com/pub/SUSE Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/c/curl/ **Mandrake:** **http://www.mandrakesecure.net/en/ftp.php** **Updates available at:** **http://curl.haxx.se/download/curl-7.13.1.tar.gz** Currently we are not aware of any exploits for these vulnerabilities.	Multiple Vendors cURL / libcURL Kerberos Authentication & 'Curl_input_ntlm()' Remote Buffer Overflows CAN-2005-0490	High	iDEFENSE Security Advisor February 21, 2005 **Mandrakelinux Security Update Advisory, MDKSA-2005:048, March 4 2005**

Multiple Vendors
Debian Linux 3.0, sparc, s/390, ppc, mipsel, mips, m68k, ia-64, ia-32, hppa, arm, alpha;
Easy Software Products CUPS 1.0.4 -8, 1.0.4, 1.1.1, 1.1.4 -5, 1.1.4 -3, 1.1.4 -2, 1.1.4, 1.1.6, 1.1.7, 1.1.10, 1.1.12-1.1.20;
Gentoo Linux;
GNOME GPdf 0.112;
KDE KDE 3.2-3.2.3, 3.3, 3.3.1, kpdf 3.2;
RedHat Fedora Core2;
Ubuntu ubuntu 4.1, ppc, ia64, ia32, Xpdf Xpdf 0.90-0.93; 1.0.1, 1.0 0a, 1.0, 2.0 3, 2.0 1, 2.0, 3.0, SUSE Linux - all versions
	Several integer overflow vulnerabilities exist in 'pdftops/Catalog.cc' and 'pdftops/XRef.cc,' which could let a remote malicious user execute arbitrary code.
	Debian:
	http://security.debian.org/pool/updates/main/c/cupsys/
	Fedora:
	http://download.fedora.redhat.com/pub/fedora/linux/core/updates/2/
	Gentoo:
	http://security.gentoo.org/glsa/glsa-200410-20.xml
	KDE:
	ftp://ftp.kde.org/pub/kde/security_patches/post-3.3.1-kdegraphics.diff
	Mandrake:
	http://www.mandrakesecure.net/en/ftp.php
	Ubuntu:
	http://security.ubuntu.com/ubuntu/pool/main/c/cupsys/
	Conectiva:
		Multiple Vendors Xpdf PDFTOPS Multiple Integer Overflows
		CAN-2004-0888
		CAN-2004-0889
			High	Security Tracker Alert ID, 1011865, October 21, 2004
				Conectiva Linux Security Announcement, CLA-2004:8 November 8, 2004
				Debian Security Advisory, D 599-1, November 25, 2004
				SUSE Security Summary Report, SUSE-SR:2004:002 November 30, 2004
				Gentoo Linux Security Advisory, GLSA 200501-31, January 23, 2005
				Fedora Update Notifications FEDORA-2005-122, 123, 133-136, February 8 & 9, 20
				Fedora Legacy Update Advisory, FLSA:2353, Febru 10, 2005
				Mandrakelinux Security Upd Advisories,

	ftp://atualizacoes.conectiva.com.br/ Debian: http://security.debian.org/pool/updates/main/t/tetex-bin/ SUSE: Update: ftp://ftp.SUSE.com/pub/SUSE Gentoo: http://security.gentoo.org/glsa/glsa-200501-31.xml Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/ FedoraLegacy: http://download.fedoralegacy.org/fedora/1/updates/ RedHat: https://rhn.redhat.com/errata/RHSA-2005-132.html **FedoraLegacy:** **http://download.fedoralegacy.org/redhat/** **RedHat:** **http://rhn.redhat.com/errata/RHSA-2005-213.html** **SGI:** **ftp://patches.sgi.com/support/free/security/advisories/** Currently we are not aware of any exploits for these vulnerabilities.			MDKSA-2005:041-044, February 18, 2005 RedHat Security Advisory, RHSA-2005:132-09, Februa 18. 2005 **Fedora Legacy Update Advisory, FLSA:2127, Mar 2, 2005** **Mandrakelinux Security Update Advisory, MDKSA-2005:052, March 4 2005** **RedHat Security Advisory, RHSA-2005:213-04, March 2005** **SGI Security Advisory, 20050204-01-U, March 7, 2**

Multiple Vendors
Debian Linux 3.0, sparc, s/390, ppc, mipsel, mips, m68k, ia-64, ia-32, hppa, arm, alpha;
Gentoo Linux;
LibTIFF LibTIFF 3.4, 3.5.1-3.5.5, 3.5.7, 3.6 .0, 3.6.1, 3.7, 3.7.1;
RedHat Fedora Core2& Core 3;
Ubuntu Ubuntu Linux 4.1 ppc, ia64, ia32;
Avaya CVLAN, Integrated Management, Intuity LX, MN100, Modular Messaging (MSS) 1.1, 2.0
	A vulnerability exists in the tiffdump utility, which could let a remote malicious user execute arbitrary code.
	Debian:
	http://security.debian.org/pool/updates/main/t/tiff/
	Fedora:
	http://download.fedora.redhat.com/pub/fedora/linux/core/updates/
	Gentoo:
	http://security.gentoo.org/glsa/glsa-200501-06.xml
	Mandrake:
	http://www.mandrakesecure.net/en/ftp.php
	SuSE:
	ftp://ftp.suse.com/pub/suse/i386/update/
	Ubuntu:
	http://security.ubuntu.com/ubuntu/pool/universe/t/tiff/
	RedHat:
	http://rhn.redhat.com/errata/RHSA-2005-019.html
	SGI:
	http://support.sgi.com/browse_request/linux_patches_by_os
	TurboLinux:
	http://www.turbolinux.com/update/
	Conectiva:
	ftp://atualizacoes.conectiva.com.br/
	Avaya:
	http://support.avaya.com/elmodocs2/security/ASA-2005-021_RHSA-2005-019.pdf
	Mandrake:
	http://www.mandrakesecure.net/en/ftp.php
	Currently we are not aware of any exploits for this vulnerability.
		LibTIFF TIFFDUMP Heap Corruption Integer Overflow
		CAN-2004-1183
			High	Security Tracker Alert ID, 1012785, January 6, 2005
				RedHat Security Advisory, RHSA-2005:019-11, Januar 13, 2005
				SGI Security Advisory, 20050101-01-U, January 19 2005
				Turbolinux Security Announcement, January 20, 2005
				Conectiva Linux Security Announcement, CLA-2005:9 January 20, 2005
				Avaya Security Advisory, ASA-2005-021, January 25, 2005
				Mandrakelinux Security Update Advisory, MDKSA-2005:052, March 4 2005

Multiple Vendors Gentoo Linux 1.4; RedHat Advanced Workstation for the Itanium Processor 2.1 IA64, 2.1, Desktop 3.0, t Enterprise Linux WS 3, WS 2.1 IA64, WS 2.1, ES 3, 2.1 IA64, 2.1, AS 3, AS 2.1 IA64, AS 2.1' Trolltech Qt 3.0, 3.0.5, 3.1, 3.1.1, 3.1.2, 3.2.1, 3.2.3, 3.3 .0, 3.3.1, 3.3.2; Avaya Intuity LX, MN100, Modular Messaging (MSS) 1.1, 2.0	Multiple vulnerabilities exist: a buffer overflow vulnerability exists in the 'read_dib()' function when handling 8-bit RLE encoded BMP files, which could let a malicious user execute arbitrary code; and buffer overflow vulnerabilities exist in the in the XPM, GIF, and JPEG image file handlers, which could let a remote malicious user execute arbitrary code. Debian: http://security.debian.org/pool/updates/main/q/qt-copy/ Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/1/ Gentoo: http://security.gentoo.org/glsa/glsa-200408-20.xml Mandrake: http://www.mandrakesecure.net/en/ftp.php Slackware: ftp://ftp.slackware.com/pub/slackware/slackware-9.0/patches/packages/kde/qt-3.1.2-i486-4.tgz SuSE: ftp://ftp.suse.com/pub/suse/i386/update Trolltech Upgrade: http://www.trolltech.com/download/index.html TurboLinux: ftp://ftp.turbolinux.com/pub/TurboLinux/TurboLinux/ia32/ Sun: http://sunsolve.sun.com/search/document.do?assetkey=1-26-57637-1&searchclause=security Conectiva: ftp://atualizacoes.conectiva.com.br/ RedHat: http://rhn.redhat.com/errata/RHSA-2004-478.html http://rhn.redhat.com/errata/RHSA-2004-479.html SuSE: ftp://ftp.suse.com/pub/suse/ Avaya: http://support.avaya.com/japple/css/japple?temp.groupID=128450&temp.selectedFamily=128451&temp.selectedProduct=154235&temp.selectedBucket=126655&temp.feedbackState=askForFeedback&temp.documentID=203389& PAGE=avaya.css.CSSLvl1Detail&executeTransaction=avaya.css.UsageUpdate() **FedoraLegacy:** **http://download.fedoralegacy.org/redhat/** Proof of Concept exploit has been published.	QT Image File Buffer Overflows CAN-2004-0691 CAN-2004-0692 CAN-2004-0693	High	Secunia Advisory, SA12325 August 10, 2004 Sun Alert ID: 57637, Septem 3, 2004 Conectiva Linux Security Announcement, CLA-2004:8 September 22, 2004 RedHat Security Advisories, RHSA-2004:478-13 & RHSA-2004:479-05, Octobe & 6, 2004 SUSE Security Announceme SUSE-SA:2004:035, Octobe 2004 Security Focus, October 18, 2004 **Fedora Legacy Update Advisory, FLSA:2314, Mar 2, 2005**
Multiple Vendors Gentoo Linux; RedHat Fedora Core3, Core2; SUSE Linux 8.1, 8.2, 9.0-9.2, Desktop 1.0, Enterprise Server 9, 8, Novell Linux Desktop 1.0; X.org X11R6 6.7 .0, 6.8, 6.8.1; XFree86 X11R6 3.3, 3.3.2-3.3.6, 4.0-4.0.3, 4.1 .0, 4.1 -12, 4.1 -11, 4.2 .0, 4.2.1 Errata, 4.2.1 4.3 .0	Multiple vulnerabilities exist due to integer overflows, memory access errors, input validation errors, and logic errors, which could let a remote malicious user execute arbitrary code, obtain sensitive information, or cause a Denial of Service. Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates Gentoo: http://security.gentoo.org/glsa/glsa-200411-28.xml SUSE: ftp://ftp.SUSE.com/pub/SUSE X.org: http://www.x.org/pub/ Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/2/ RedHat: http://rhn.redhat.com/errata/	Multiple Vendors LibXPM Multiple Vulnerabilities CAN-2004-0914	Low/ Medium/ High (Low if a DoS; Medium if sensitive information can be obtained; and High if arbitrary code can be executed)	X.Org Foundation Security Advisory, November 17, 200 Fedora Update Notifications FEDORA-2004-433 & 434, November 17 & 18, 2004 SUSE Security Announceme SUSE-SA:2004:041, Novem 17, 2004 Gentoo Linux Security Advisory, GLSA 200411-28, November 19, 2004 Fedora Security Update Notifications FEDORA-2003-464, 465, 46 & 467, December 1, 2004 RedHat Security Advisory, RHSA-2004:537-17, Decem 2, 2004

	RHSA-2004-537.html Mandrakesoft: http://www.mandrakesoft.com/security/advisories?name=MDKSA-2004:137 (libxpm) http://www.mandrakesoft.com/security/advisories?name=MDKSA-2004:138 (XFree86) Debian: http://www.debian.org/security/2004/dsa-607 (XFree86) SGI: ftp://patches.sgi.com/support/free/security/patches/ProPack/3/ TurboLinux: http://www.turbolinux.com/update/ Avaya: http://support.avaya.com/elmodocs2/security/ASA-2005-023_RHSA-2004-537.pdf http://support.avaya.com/elmodocs2/security/ASA-2005-025_RHSA-2005-004.pdf Gentoo: http://security.gentoo.org/glsa/glsa-200502-06.xml http://security.gentoo.org/glsa/glsa-200502-07.xml Ubuntu: http://security.ubuntu.com/ubuntu/pool/ **FedoraLegacy:** **http://download.fedoralegacy.org/redhat/** Currently we are not aware of any exploits for these vulnerabilities.		Mandrakesoft: MDKSA-2004:137: libxpm4; MDKSA-2004:138: XFree86 November 22, 2004 Debian Security Advisory DSA-607-1 xfree86 -- severa vulnerabilities, December 10 2004 Turbolinux Security Announcement, January 20, 2005 Avaya Security Advisories, ASA-2005-023 & 025, Janua 25, 2005 Gentoo Linux Security Advisories, GLSA 200502-0 07, February 7, 2005 Ubuntu Security Notice, USN-83-1 February 16, 200 **Fedora Legacy Update** **Advisory, FLSA:2314, Mar** **2, 2005**

Multiple Vendors Linux kernel 2.2-2.2.2.27 -rc1, 2.4-2.4.29 -rc1, 2.6 .10, 2.6- 2.6.10	A race condition vulnerability exists in the page fault handler of the Linux Kernel on symmetric multiprocessor (SMP) computers, which could let a malicious user obtain superuser privileges. Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/ Trustix: ftp://ftp.trustix.org/pub/trustix/updates/ Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/l/ SuSE: ftp://ftp.suse.com/pub/suse/ RedHat: http://rhn.redhat.com/errata/RHSA-2005-016.html http://rhn.redhat.com/errata/RHSA-2005-017.html Mandrake: http://www.mandrakesecure.net/en/ftp.php RedHat: https://rhn.redhat.com/errata/RHSA-2005-092.html FedoraLegacy: http://download.fedoralegacy.org/redhat/ SuSE: ftp://ftp.suse.com/pub/suse/ TurboLinux: ftp://ftp.turbolinux.co.jp/pub/TurboLinux/TurboLinux/ **Conectiva:** **ftp://atualizacoes.conectiva.com.br/** Exploit scripts have been published.	Linux Kernel Symmetrical Multiprocessing Page Fault Superuser Privileges CAN-2005-0001	High	Security Tracker Alert, 1012862, January 12, 2005 SUSE Security Announceme SUSE-SA:2005:003, Januar 21, 2005 RedHat Security Advisory, RHSA-2005:016-13 & 017-1 January 21, 2005 Mandrake Security Advisory MDKSA-2005:022, January 2005 RedHat Security Advisory, RHSA-2005:092-14, Februa 18, 2005 Fedora Legacy Update Advisory, FLSA:2336, Febru 24, 2005 SUSE Security Announceme SUSE-SA:2005:010, Februa 25, 2005 Turbolinux Security Announcement , February 2 2005 **Conectiva Linux Security Announcement, CLA-2005:930, March 7, 20**
Multiple Vendors Linux kernel 2.4 .0-test1-test12, 2.4-2.4.28, 2.4.29rc1&rc2, 2.5 .0-2.5.69, 2.6 -test1-test11, 2.6-2.6.10; SuSE . Linux 8.1, 8.2, 9.0	A Denial of Service vulnerability exists with Direct I/O access to NFS file systems. SuSE: ftp://ftp.suse.com/pub/suse/ **Conectiva:** **ftp://atualizacoes.conectiva.com.br/** Currently we are not aware of any exploits for this vulnerability.	Linux Kernel NFS I/O Denial of Service CAN-2005-0207	Low	SUSE Security Announceme SUSE-SA:2005:003, Januar 21, 2005 **Conectiva Linux Security Announcement, CLA-2005:930, March 7, 20**
Multiple Vendors Linux Kernel 2.4.0 test1-test12, 2.4-2.4.28, 2.4.29 -rc2, 2.6, test1-test11, 2.6.1, rc1-rc2, 2.6.2-2.6.9, 2.6.10 rc2; Avaya S8710/S8700/ S8500/S8300, Converged Communication Server, Intuity LX, MN100, Modular Messaging, Network Routing	A vulnerability exists in the 'load_elf_library()' function in 'binfmt_elf.c' because memory segments are not properly processed, which could let a remote malicious user execute arbitrary code with root privileges. Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/ Trustix: http://http.trustix.org/pub/trustix/updates/ Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/l/ Mandrake: http://www.mandrakesecure.net/en/ftp.php Avaya: http://support.avaya.com/elmodocs2/security/ASA-2005-034_RHSA-2005-016RHSA-2006-017RHSA-2005-043.pdf Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.8.1/ RedHat:	Linux Kernel uselib() Root Privileges CAN-2004-1235	High	iSEC Security Research Advisory, January 7, 2005 Fedora Update Notifications FEDORA-2005-013 & 014, January 10, 2005 Trustix Secure Linux Securit Advisory, TSLSA-2005-0001 January 13, 2005 Mandrake Security Advisory MDKSA-2005:022, January 2005 PacketStorm, January 27, 2 Avaya Security Advisory, ASA-2005-034, February 8, 2005 Ubuntu Security Notice, USN-57-1, February 9, 2005 RedHat Security Advisory, RHSA-2005:092-14, Februa 18, 2005 Fedora Legacy Update

	https://rhn.redhat.com/errata/RHSA-2005-092.html FedoraLegacy: http://download.fedoralegacy.org/redhat/ TurboLinux: ftp://ftp.turbolinux.co.jp/pub/TurboLinux/TurboLinux/ **Conectiva:** **ftp://atualizacoes.conectiva.com.br/** Another exploit script has been published.			Advisory, FLSA:2336, Febru 24, 2005 SUSE Security Announcem SUSE-SA:2005:010, Februa 25, 2005 Turbolinux Security Announcement , February 2 2005 **Conectiva Linux Security Announcement, CLA-2005:930, March 7, 20**
Multiple Vendors Linux kernel 2.6.10, 2.6 -test9-CVS, 2.6-test1- -test11, 2.6, 2.6.1-2.6.11 ; RedHat Desktop 4.0, Enterprise Linux WS 4, ES 4, AS 4	Multiple vulnerabilities exist: a vulnerability exists in the 'shmctl' function, which could let a malicious user obtain sensitive information; a Denial of Service vulnerability exists in 'nls_ascii.c' due to the use of incorrect table sizes; a race condition vulnerability exists in the 'setsid()' function; and a vulnerability exists in the OUTS instruction on the AMD64 and Intel EM64T architecture, which could let a malicious user obtain elevated privileges. RedHat: https://rhn.redhat.com/errata/RHSA-2005-092.html Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.8.1/ FedoraLegacy: http://download.fedoralegacy.org/redhat/ **Conectiva:** **ftp://atualizacoes.conectiva.com.br/** Currently we are not aware of any exploits for these vulnerabilities.	Linux Kernel Multiple Vulnerabilities CAN-2005-0176 CAN-2005-0177 CAN-2005-0178 CAN-2005-0204	Low/Medium (Low if a DoS)	Ubuntu Security Notice, USN-82-1, February 15, 200 RedHat Security Advisory, RHSA-2005:092-14, Februa 18, 2005 Fedora Legacy Update Advisory, FLSA:2336, Febru 24, 2005 **Conectiva Linux Security Announcement, CLA-2005:930, March 7, 20**
Multiple Vendors Linux kernel 2.6.x, 2.4.x , SUSE Linux 8.1, 8.2, 9.0, 9.1, Linux 9.2, SUSE Linux Desktop 1.x, SUSE Linux Enterprise Server 8, 9; Turbolinux Turbolinux Server 10.0	Two vulnerabilities exist: a Denial of Service vulnerability exists via a specially crafted 'a.out' binary; and a vulnerability exists due to a race condition in the memory management, which could let a malicious user obtain sensitive information. SUSE: http://www.SUSE.de/de/security/2004_42_kernel.html TurboLinux: ftp://ftp.turbolinux.co.jp/pub/TurboLinux/TurboLinux/ia32/Server/10/updates/RPMS/ Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/ Trustix: http://http.trustix.org/pub/trustix/updates/ Mandrake: http://www.mandrakesecure.net/en/ftp.php FedoraLegacy: http://download.fedoralegacy.org/redhat/ **Conectiva:** **ftp://atualizacoes.conectiva.com.br/** Currently we are not aware of any exploits for these vulnerabilities.	Multiple Vendors Linux Kernel Local DoS & Memory Content Disclosure CAN-2004-1074	**Low/ Medium** **(Medium if sensitive information can be obtained)**	Secunia Advisory, SA13308, November 25, 20 SUSE Security Summary Report, SUSE-SA:2004:042 December 1, 2004 Security Focus, December 1 2004 Trustix Secure Linux Securit Advisory, TSLSA-2005-0001 January 13, 2005 Mandrake Security Advisory MDKSA-2005:022, January 2005 Fedora Legacy Update Advisory, FLSA:2336, Febru 24, 2005 **Conectiva Linux Security Announcement, CLA-2005:930, March 7, 20**
Multiple Vendors nfs-utils 1.0.6	A vulnerability exists due to an error in the NFS statd server in 'statd.c' where the 'SIGPIPE' signal is not correctly ignored. This can be exploited to crash a vulnerable service via a malicious peer terminating a TCP connection prematurely. Upgrade to 1.0.7-pre1: http://sourceforge.net/project/showfiles.php?group_id=14&package_id=174 Mandrakesoft: http://www.mandrakesoft.com/security/advisories?name=MDKSA-2004:146 Debian: http://www.debian.org/security/2004/dsa-606 Red Hat: http://rhn.redhat.com/errata/RHSA-2004-583.html Mandrake:	Multiple Vendors nfs-utils 'SIGPIPE' TCP Connection Termination Denial of Service CAN-2004-0946 CAN-2004-1014	Low	Secunia Advisory ID, SA133 December 7, 2004 Debian Security Advisory DSA-606-1 nfs-utils, Decem 8, 2004 Red Hat Security Advisory, RHSA-2004:583-09, Decem 20, 2004 Mandrakelinux Security Upd Advisory, MDKSA-2005:005 January 12, 2005 **US-CERT VU#698302**

	http://www.mandrakesecure.net/en/ftp.php Currently we are not aware of any exploits for this vulnerability.			
Multiple Vendors Samba 2.2.9, 3.0.8 and prior	An integer overflow vulnerability in all versions of Samba's smbd 0.8 could allow an remote malicious user to cause controllable heap corruption, leading to execution of arbitrary commands with root privileges. Patches available at: http://www.samba.org/samba/ftp/patches/security/samba-3.0.9-CAN-2004-1154.patch Red Hat: http://rhn.redhat.com/errata/RHSA-2004-670.html Gentoo: http://www.gentoo.org/security/en/glsa/glsa-200412-13.xml Trustix: http://www.trustix.net/errata/2004/0066/ Red Hat (Updated): http://rhn.redhat.com/errata/RHSA-2004-670.html Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/ SUSE: http://www.novell.com/linux/security/advisories/2004_45_samba.html Mandrakesoft: http://www.mandrakesoft.com/security/advisories?name=MDKSA-2004:158 Conectiva: ftp://atualizacoes.conectiva.com.br/ RedHat: http://rhn.redhat.com/errata/RHSA-2005-020.html HP: http://software.hp.com TurboLinux: ftp://ftp.turbolinux.co.jp/pub/TurboLinux/TurboLinux/ia32/ **SCO:** **ftp://ftp.sco.com/pub/updates/UnixWare/SCOSA-2005.17** Currently we are not aware of any exploits for this vulnerability.	Multiple Vendors Samba smbd Security Descriptor CAN-2004-1154	High	iDEFENSE Security Advisor 12.16.04 Red Hat Advisory, RHSA-2004:670-10, Decem 16, 2004 Gentoo Security Advisory, GLSA 200412-13 / Samba, December 17, 2004 US-CERT, Vulnerability Note VU#226184, December 17, 2004 Trustix Secure Linux Adviso #2004-0066, December 17, 2004 Red Hat, RHSA-2004:670-1 December 16, 2004 SUSE, SUSE-SA:2004:045, December 22, 2004 RedHat Security Advisory, RHSA-2005:020-04, Januar 2005 Conectiva Linux Security Announcement, CLA-2005:913,January 6, 20 Turbolinux Security Announcement, February 7, 2005 HP Security Advisory, HPSBUX01115, February 3 2005 **SCO Security Advisory, SCOSA-2005.17, March 7, 2005**

Multiple Vendors Squid 2.x; Gentoo Linux;Ubuntu Linux 4.1 ppc, ia64, ia32;Ubuntu Linux 4.1 ppc, ia64, ia32; Conectiva Linux 9.0, 10.0	A remote Denial of Service vulnerability exists in the NTLM fakeauth_auth helper when running under a high load or for a long period of time, and a specially crafted NTLM type 3 message is submitted. Patch available at: http://www.squid-cache.org/Versions/v2/2.5/bugs/squid-2.5.STABLE7-fakeauth_auth.patch Gentoo: http://security.gentoo.org/glsa/glsa-200501-25.xml Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/ Conectiva: ftp://atualizacoes.conectiva.com.br/ Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates RedHat: http://rhn.redhat.com/errata/RHSA-2005-061.html SUSE: ftp://ftp.suse.com/pub/suse/ Trustix: http://www.trustix.org/errata/2005/0003/ **Astaro:** **http://www.astaro.org/showflat.php?Cat=&Number=56136&page=0&view=collapsed&sb=5&o=&fpart=1#56136** Currently we are not aware of any exploits for this vulnerability.	Squid NTLM fakeauth_auth Helper Remote Denial of Service CAN-2005-0096	Low	Secunia Advisory, SA13789, January 11, 2005 Gentoo Linux Security Advis GLSA 200501-25, January 1 2005 Ubuntu Security Notice, USN-67-1, January 20, 2005 Conectiva Linux Security Announcement, CLA-2005:9 January 26, 2005 Fedora Update Notifications FEDORA-2005-105 & 106, February 1, 2005 SUSE Security Summary Report, SUSE-SR:2005:003 February 4, 2005 SUSE Security Announceme SUSE-SA:2005:006, Februa 10, 2005 Trustix Secure Linux Securit Advisory, TSLSA-2005-0003 February 11, 2005 RedHat Security Advisory, RHSA-2005:061-19, Februa 11, 2005 **Security Focus, 12324, Ma 7, 2005**
Multiple Vendors X.org X11R6 6.7.0, 6.8, 6.8.1; XFree86 X11R6 3.3, 3.3.2-3.3.6, 4.0, 4.0.1, 4.0.2 -11, 4.0.3, 4.1.0, 4.1 -12, 4.1 -11, 4.2 .0, 4.2.1 Errata, 4.2.1, 4.3.0.2, 4.3.0.1, 4.3.0	An integer overflow vulnerability exists in 'scan.c' due to insufficient sanity checks on on the 'bitmap_unit' value, which could let a remote malicious user execute arbitrary code. Patch available at: https://bugs.freedesktop.org/attachment.cgi?id=1909 Gentoo: http://security.gentoo.org/glsa/glsa-200503-08.xml Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/l/lesstif1-1/ Currently we are not aware of any exploits for this vulnerability.	LibXPM Bitmap_unit Integer Overflow CAN-2005-0605	High	Security Focus, 12714, Marc 2, 2005 Gentoo Linux Security Advisory, GLSA 200503-08, March 4, 2005 Ubuntu Security Notice, USN-92-1 March 07, 2005
Multiple Vendors xli 1.14-1.17	A vulnerability exists due to a failure to manage internal buffers securely, which could let a remote malicious user execute arbitrary code. No workaround or patch available at time of publishing. Currently we are not aware of any exploits for this vulnerability.	XLI Internal Buffer Management CAN-2005-0639	High	Gentoo Linux Security Advisory, GLSA 200503-05, March 2, 2005
Multiple Vendors xli 1.14-1.17; xloadimage 3.0, 4.0, 4.1	A vulnerability exists due to a failure to parse compressed images safely, which could let a remote malicious user execute arbitrary code. Gentoo: http://security.gentoo.org/glsa/glsa-200503-05.xml Currently we are not aware of any exploits for this vulnerability.	XLoadImage Compressed Image Remote Command Execution CAN-2005-0638	High	Gentoo Linux Security Advisory, GLSA 200503-05, March 2, 2005
Open Group Open Motif 2.x, Motif 1.x; Avaya CMS Server 8.0, 9.0, 11.0, CVLAN, Integrated Management, Intuity LX, MN100, Modular Messaging (MSS) 1.1, 2.0, Network Routing	Multiple vulnerabilities have been reported in Motif and Open Motif, which potentially can be exploited by malicious people to compromise a vulnerable system. Updated versions of Open Motif and a patch are available. A commercial update will also be available for Motif 1.2.6 for users, who have a commercial version of Motif. http://www.ics.com/developers/index.php?cont=xpm_security_alert Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/2/ Red Hat: http://rhn.redhat.com/errata/	Open Group Motif / Open Motif libXpm Vulnerabilities CAN-2004-0687 CAN-2004-0688	High	Integrated Computer Solutio Secunia Advisory ID: SA133 December 2, 2004 RedHat Security Advisory: RHSA-2004:537-17, Decem 2, 2004 Turbolinux Security Announcement, January 20, 2005 Avaya Security Advisories, ASA-2005-023 & 025, Janua

	RHSA-2004-537.html Gentoo: http://security.gentoo.org/glsa/glsa-200410-09.xml Debian: http://security.debian.org/pool/updates/main/i/imlib/ Mandrake: http://www.mandrakesecure.net/en/ftp.php SuSE: ftp://ftp.suse.com/pub/suse/ Ubuntu: http://security.ubuntu.com/ubuntu/pool/universe/x/xfree86/ TurboLinux: http://www.turbolinux.com/update/ Avaya: http://support.avaya.com/elmodocs2/security/ASA-2005-023_RHSA-2004-537.pdf http://support.avaya.com/elmodocs2/security/ASA-2005-025_RHSA-2005-004.pdf Gentoo: http://security.gentoo.org/glsa/glsa-200502-07.xml Conectiva: http://distro.conectiva.com.br/atualizacoes/index.php?id=a&anuncio=000924 **FedoraLegacy:** **http://download.fedoralegacy.org/redhat/** Currently we are not aware of any exploits for these vulnerabilities.			25, 2005 SUSE Security Summary Report, SUSE-SR:2005:003 February 4, 2005 Gentoo Linux Security Advisory, GLSA 200502-07, February 7, 2005 Conectiva Security Advisory CLSA-2005:924, February 1 2005 **Fedora Legacy Update Advisory, FLSA:2314, Mar 2, 2005**
OpenBSD OpenBSD 3.5, 3.6	A vulnerability exists in 'sys/arch/i386/i386/locore.s' in the copy(9) function due to improper checking functions. The impact was not specified. Patches available at: ftp://ftp.openbsd.org/pub/OpenBSD/patches/3.5/i386/028_locore.patch ftp://ftp.openbsd.org/pub/OpenBSD/patches/3.6/i386/011_locore.patch Currently we are not aware of any exploits for this vulnerability.	OpenBSD copy(9) Function CAN-2005-0637	Not Specified	Security Tracker Alert, 1013333, March 1, 2005
RedHat Linux 9.0 i386	A buffer overflow vulnerability exists due to insecure copying of file data into finite process buffers, which could let a remote malicious user execute arbitrary code. Upgrade available at: http://download.fedoralegacy.org/redhat/9/updates/i386/less-378-7.2.legacy.i386.rpm Currently we are not aware of any exploits for this vulnerability.	RedHat Linux Remote Buffer Overflow CAN-2005-0086	High	Fedora Legacy Update Advisory, FLSA:2404, March 2005

Remote Sensing LibTIFF 3.5.7, 3.6.1, 3.7.0; Avaya CVLAN, Integrated Management, Intuity LX, MN100, Modular Messaging (MSS) 1.1, 2.0	Two vulnerabilities exist which can be exploited by malicious people to compromise a vulnerable system by executing arbitrary code. The vulnerabilities are caused due to an integer overflow in the "TIFFFetchStripThing()" function in "tif_dirread.c" when parsing TIFF files and"CheckMalloc()" function in "tif_dirread.c" and "tif_fax3.c" when handling data from a certain directory entry in the file header. Update to version 3.7.1: ftp://ftp.remotesensing.org/pub/libtiff/ Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/ Debian: http://www.debian.org/security/2004/dsa-617 Gentoo: http://security.gentoo.org/glsa/glsa-200501-06.xml Mandrake: http://www.mandrakesecure.net/en/ftp.php SUSE: ftp://ftp.suse.com/pub/suse/ RedHat: http://rhn.redhat.com/errata/RHSA-2005-019.html SGI: http://support.sgi.com/browse_request/linux_patches_by_os TurboLinux: http://www.turbolinux.com/update/ Conectiva: ftp://atualizacoes.conectiva.com.br/ Avaya: http://support.avaya.com/elmodocs2/security/ASA-2005-021_RHSA-2005-019.pdf **Mandrake:** **http://www.mandrakesecure.net/en/ftp.php** Currently we are not aware of any exploits for these vulnerabilities.	Remote Sensing LibTIFF Two Integer Overflow Vulnerabilities CAN-2004-1308	High	iDEFENSE Security Advisor 12.21.04 Secunia SA13629, Decemb 23, 2004 SUSE Security Announcem SUSE-SA:2005:001, Januar 10, 2005 RedHat Security Advisory, RHSA-2005:019-11, Januar 13, 2005 US-Cert Vulnerability Note, VU#125598, January 14, 20 SGI Security Advisory, 20050101-01-U, January 19 2005 Turbolinux Security Announcement, January 20, 2005 Conectiva Linux Security Announcement, CLA-2005:9 January 20, 2005 Avaya Security Advisory, ASA-2005-021, January 25, 2005 **Mandrakelinux Security Update Advisory, MDKSA-2005:052, March 4 2005**
Rob Flynn Gaim 1.0-1.0.2, 1.1.1, 1.1.2	Multiple remote Denial of Service vulnerabilities exist: a vulnerability exists when a remote malicious ICQ or AIM user submits certain malformed SNAC packets; and a vulnerability exists when parsing malformed HTML data. Upgrades available at: http://gaim.sourceforge.net/downloads.php Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/ Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/g/gaim/ **Gentoo:** **http://security.gentoo.org/glsa/glsa-200503-03.xml** **Mandrake:** **Http://www.mandrakesecure.net/en/advisories/** There is no exploit code required.	Gaim Multiple Remote Denials of Service CAN-2005-0472 CAN-2005-0473	Low	Gaim Advisory, February 17 2005 Fedora Update Notifications FEDORA-2005-159 & 160, February 21, 2005 US-CERT VU#839280 US-CERT VU#523888 Ubuntu Security Notice, USN-85-1 February 25, 200 **Gentoo Linux Security Advisory, GLSA 200503-0 March 1, 2005** **Mandrakelinux Security Update Advisory, MDKSA-2005:049, March 4 2005**
server-side.de HTTP Anti Virus Proxy prior to 0.51	A vulnerability exists due to a failure to detect known viruses in cab and zip archives. Update available at: http://www.bemberg.de/server-side/download.htm Currently we are not aware of any exploits for this vulnerability.	HTTP Anti Virus Proxy Virus Detection CAN-2005-0668	Medium	Security Tracker Alert, 1013370, March 4, 2005

Squid-cache.org Squid Web Proxy Cache 2.5 .STABLE5-STABLE8	A remote Denial of Service vulnerability exists when performing a Fully Qualify Domain Name (FQDN) lookup and and unexpected response is received. Patches available at: http://downloads.securityfocus.com/vulnerabilities/patches/ Gentoo: http://security.gentoo.org/glsa/glsa-200502-25.xml Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/ Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/ SUSE: ftp://ftp.SUSE.com/pub/SUSE Debian: http://security.debian.org/pool/updates/main/s/squid/ Mandrake: http://www.mandrakesecure.net/en/ftp.php **RedHat:** **http://rhn.redhat.com/errata/RHSA-2005-173.html** Currently we are not aware of any exploits for this vulnerability.	Squid Proxy FQDN Remote Denial of Service CAN-2005-0446	Low	Secunia Advisory, SA14271, February 14, 200 Gentoo Linux Security Advis GLSA, 200502-25, February 18, 2005 Ubuntu Security Notice, USN-84-1, February 21, 200 Fedora Update Notifications FEDORA-2005-153 & 154, February 21, 2005 SUSE Security Announceme SUSE-SA:2005:008, Februa 21, 2005 Debian Security Advisory, D 688-1, February 23, 2005 Mandrakelinux Security Upd Advisory, MDKSA-2005:047 February 24, 2005 **RedHat Security Advisory, RHSA-2005:173-09, March 2005**
Sun Microsystems, Inc. AnswerBook2 1.2-1.4.4	Multiple Cross-Site Scripting vulnerabilities exist: a vulnerability exists in the 'Search' function and the 'AnswerBook2 admin' interface due to insufficient sanitization of user-supplied data, which could let a remote malicious user execute arbitrary HTML and script code. Workaround available at: http://sunsolve.sun.com/search/document.do?assetkey=1-26-577371&searchclause=%22category:security%22%20%22availability,%20security%22 There is no exploit code required.	Sun Solaris AnswerBook2 Multiple Cross-Site Scripting CAN-2005-0548 CAN-2005-0549	High	Sun(sm) Alert Notification, S Alert ID: 57737, March 7, 20
Symantec Enterprise Firewall 8.0	A vulnerability exists win the integrated DNS proxy when acting as a caching DNS server, which could let a remote malicious user deny service to legitimate users by redirecting traffic to inappropriate hosts, perform man-in-the-middle attacks, and impersonate sites. Updates available at: http://securityresponse.symantec.com/avcenter/security/Content/2004.06.21.html **Hotfixes available at:** **http://service1.symantec.com/support/ent-gate.nsf/docid/2005030417285454** Proof of Concept exploit scripts have been published.	Symantec Enterprise Firewall DNSD DNS Cache Poisoning CAN-2004-1754	Medium	Symantec Security Advisory SYM04-010, June 21, 2004 **Security Focus, 10557, Ma 6, 2005**
The PaX Team PaX linux 2.6.5, 2.4.20-2.4.28, 2.2.x	A vulnerability exists due to an undisclosed error, which could let a malicious user obtain elevated privileges and execute arbitrary code. Patches available at: http://pax.grsecurity.net/pax-linux-2.6.11-200503050030.patch Currently we are not aware of any exploits for this vulnerability.	PaX Undisclosed Arbitrary Code Execution CAN-2005-0666	High	Security Focus, 12729, Marc 4, 2005
Trolltech Qt 3.0, 3.0.3, 3.0.5, 3.1-3.1.2, 3.2.1, 3.2.3, 3.3.0-3.3.4	A vulnerability exists due to a failure to secure local dynamically loaded libraries, which could let a malicious user execute arbitrary code. Gentoo: http://security.gentoo.org/glsa/glsa-200503-01.xml There is no exploit code required.	Trolltech QT Arbitrary Code Execution CAN-2005-0627	High	Gentoo Linux Security Advisory, GLSA 200503-01, March 1, 2005

University of Washington imap 2004b, 2004a, 2004, 2002b-2002e	A vulnerability exists due to a logic error in the Challenge-Response Authentication Mechanism with MD5 (CRAM-MD5) code, which could let a remote malicious user bypass authentication. Update available at: ftp://ftp.cac.washington.edu/ mail/imap-2004b.tar.Z Gentoo: http://security.gentoo.org/ glsa/glsa-200502-02.xml Mandrake: http://www.mandrakesecure.net/ en/ftp.php RedHat: http://rhn.redhat.com/ errata/RHSA-2005-128.html SUSE: ftp://ftp.SUSE.com/pub/SUSE **SGI:** **ftp://oss.sgi.com/projects/sgi_ propack/download/3/updates/** Currently we are not aware of any exploits for this vulnerability.	University Of Washington IMAP Server CRAM-MD5 Remote Authentication Bypass CAN-2005-0198	Medium	US-CERT VU#702777, Janu 27, 2005 Gentoo Linux Security Advisory, GLSA 200502-02, February 2, 2005 Mandrakelinux Security Upd Advisory, MDKSA-2005:026 February 2, 2005 RedHat Security Advisory, RHSA-2005:128-06, Februa 23, 2005 SUSE Security Announcements, SUSE-SR:2005:006 & SUSE-SA:2005:012, Februa 25 & March 1, 2005 **SGI Security Advisory, 20050301-01-U, March 7, 2**
VIM Development Group VIM 6.0-6.2, 6.3.011, 6.3.025, 6.3 .030, 6.3.044, 6.3 .045	Multiple vulnerabilities exist in 'tcltags' and 'vimspell.sh' due to the insecure creation of temporary files, which could let a malicious user corrupt arbitrary files. Ubuntu: http://security.ubuntu.com/ubuntu/ pool/main/v/vim/ Mandrake: http://www.mandrakesecure.net /en/ftp.php RedHat: http://rhn.redhat.com/errata/ RHSA-2005-122.html Fedora: http://download.fedoralegacy.org/ redhat/ **SGI:** **ftp://oss.sgi.com/projects/sgi_ propack/download/3/updates/** There is no exploit required.	Vim Insecure Temporary File Creation CAN-2005-0069	Medium	Secunia Advisory, SA13841, January 13, 2005 Ubuntu Security Notice, USN-61-1, January 18, 2005 Mandrakelinux Security Upd Advisory, MDKSA-2005:026 February 2, 200 Fedora Legacy Update Advisory, FLSA:2343, Febru 24, 2005 **SGI Security Advisory, 20050204-01-U, March 7, 2**
XFree86 Project OpenBSD; xdm CVS	A vulnerability exists in xdm because even though 'DisplayManager.requestPort' is set to 0 xdm will open a 'chooserFd' TCP socket on all interfaces, which could lead to a false sense of security. Patch available at: ftp://ftp.openbsd.org/pub/OpenBSD/ patches/3.5/common/008_xdm.patch Gentoo: http://security.gentoo.org/glsa/ glsa-200407-05.xml Mandrake: http://www.mandrakesecure.net/en/ftp.php RedHat: http://rhn.redhat.com/errata/ RHSA-2004-478.html **FedoraLegacy:** **http://download.fedoralegacy. org/redhat/** Currently we are not aware of any exploits for this vulnerability.	XFree86 XDM RequestPort False Sense of Security CAN-2004-0419	Medium	Secunia Advisory, SA11723 May 30, 2004 RedHat Security Advisory, RHSA-2004:478-13, Octobe 2004 **Fedora Legacy Update Advisory, FLSA:2314, Mar 2, 2005**

[back to top]

Multiple Operating Systems - Windows / UNIX / Linux / Other

Vendor & Software Name	Vulnerability - Impact Patches - Workarounds Attacks Scripts	Common Name / CVE Reference	Risk	Source

Apache mod_python	A vulnerability exists in mod_python in the publisher handler that could permit a remote malicious user to view certain python objects. A remote user can submit a specially crafted URL to view the names and values of variables. Red Hat: http://rhn.redhat.com/errata/RHSA-2005-104.html Ubuntu: http://www.ubuntulinux.org/support/documentation/usn/usn-80-1 Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates Gentoo: http://www.gentoo.org/security/en/glsa/glsa-200502-14.xml Trustix: http://www.trustix.org/errata/2005/0003/ Debian: http://www.debian.org/security/2005/dsa-689 **Conectiva:** **http://distro.conectiva.com.br/atualizacoes/index.php?id=a&anuncio=000926** Currently we are not aware of any exploits for this vulnerability.	Apache mod_python Information Disclosure Vulnerability CAN-2005-0088	Medium	Security Tracker Alert ID, 1013156, February 11, 2005 Red Hat RHSA-2005:104-03, February 10, 2005 Ubuntu, USN-80-1 February 11, 2005 Trustix #2005-0003, February 11, 2005 Debian, DSA-689-1, February 23, 2005 **Conectiva CLSA-2005:926, March 2, 2005**
Appalachian State University phpWebSite 0.10.0 and prior	A vulnerability exists in the Announce module that could let a remote malicious user who has privileges to upload image files execute arbitrary commands. No workaround or patch available at time of publishing. **Gentoo:** **http://security.gentoo.org/glsa/glsa-200503-04.xml** A Proof of Concept exploit has been published.	Appalachian State phpWebSite Arbitrary Code Execution Vulnerability CAN-2005-0565	High	Security Focus, Bugtraq ID: 12653, February 25, 2005 **Gentoo, GLSA 200503-04, March 1, 2005**
auraCMS auraCMS 1.5	Multiple vulnerabilities exist that could let a remote malicious user conduct Cross-Site Scripting attacks or determine the installation path. This is due to input validation errors in various parameters. No workaround or patch available at time of publishing. A Proof of Concept exploit has been published.	auraCMS Discloses Path to Remote Users and Permits Cross-Site Scripting Attacks CAN-2005-0655 CAN-2005-0656	High	Security Tracker Alert ID: 1013357, March 2 2005
Aztek Forum 4.0	An authentication vulnerability exists that could let a remote malicious user obtain a backup file. This is because of an authentication error in the 'myadmin.php' script. No workaround or patch available at time of publishing. A Proof of Concept exploit script has been published.	Aztek Forum Information Disclosure Vulnerability CAN-2005-0700	Low	Security Focus, Bugtraq ID 12745, March 7 2005
Bfriendly.com Einstein 1.x	A vulnerability exists that could permit local malicious users to access sensitive information. This is because user credentials are stored in plain text. No workaround or patch available at time of publishing. Currently we are not aware of any exploits for this vulnerability.	Bfriendly.com Einstein Information Disclosure Vulnerability CAN-2005-0620	Medium	Secunia SA14455, March 2, 2005
Carsten Fuchs Carsten's 3D Engine (Ca3DE) March 2004 and prior version	Two vulnerabilities exist that could let a remote malicious user cause the game service to crash or execute arbitrary code. This is caused when a command containing certain format string characters are executed. A text string that is not NULL can also cause a Denial of Service. No workaround or patch available at time of publishing. A Proof of Concept exploit has been published.	Carsten's 3D Engine Remote Code Execution Vulnerability CAN-2005-0671 CAN-2005-0672	Low/High (High if arbitrary code can be executed)	Security Tracker Alert ID: 1013361, March 3, 2005
COINSoft Technologies phpCOIN 1.2.0, 1.2.1, 1.2.1b	A vulnerability exists that could permit a remote malicious user to inject SQL commands and conduct Cross-Site Scripting attacks. This is due to input validation errors in the 'mod.php' and 'login.php' scripts.	COINSoft Technologies phpCOIN Input Validation	High	Secunia, SA14439, March 1, 2005

	No workaround or patch available at time of publishing. A Proof of Concept exploit has been published.	Vulnerabilities CAN-2005-0669 CAN-2005-0670		
Computer Associates License 1.53 - 1.61.8	Multiple buffer overflow vulnerabilities exist that could let a remote malicious user execute arbitrary code with root level privileges. A remote user can also create files in arbitrary locations on the target system. This is because of input validation errors PUTOLF requests, GETCONFIG, and GCR requests. A fixed version (1.61.9) is available at: http://supportconnectw.ca.com/public/reglic/downloads/licensepatch.asp#alp An exploit script has been published.	Computer Associates License Remote Code Execution Vulnerability CAN-2005-0581 CAN-2005-0582 CAN-2005-0583	High	iDEFENSE, 03.02.05
demof Forumwa v1	An input validation vulnerability exists that could let a remote malicious user conduct Cross-Site Scripting attacks. There is an input validation error in the 'search.php' script. No workaround or patch available at time of publishing. A Proof of Concept exploit has been published.	demof Forumwa Input Validation Vulnerabilities CAN-2005-0628	High	Hackerlounge Research Group, HRG005, March 1, 2005
D-forum 1.11	Multiple vulnerabilities exist that could let a remote malicious user conduct Cross-Site Scripting attacks. There are input validation errors in a number of different fields. No workaround or patch available at time of publishing. A Proof of Concept exploit has been published.	D-forum Input Validation Vulnerabilities CAN-2005-0660	High	Security Tracker Alert ID: 1013349, March 2, 2005
Drupal prior to 4.5.2	A vulnerability exists that could let remote malicious users conduct Cross-Site Scripting attacks. This ids due to improper input validation. Update to version 4.5.2: http://drupal.org/drupal-4.5.2 A Proof of Concept exploit has been published.	Drupal Unspecified Cross-Site Scripting Vulnerability CAN-2005-0682	High	Security Focus, Bugtraq ID 12757, March 8, 2005
Ethereal Group Ethereal 0.10-0.10.8	A buffer overflow vulnerability exists due to a failure to copy network derived data securely into sensitive process buffers, which could let a remote malicious user execute arbitrary code. No workaround or patch available at time of publishing. An exploit script has been published.	Ethereal Buffer Overflow CAN-2005-0699	High	Security Focus, 12759, March 8, 2005
Foxmail Server 2.0	Multiple vulnerabilities exist that could let a remote malicious user execute arbitrary code or cause a Denial of Service on the target system. This is because the POP server does not properly validate input in the 'USER' command. No workaround or patch available at time of publishing. Currently we are not aware of any exploits for these vulnerabilities.	Foxmail Remote Code Execution Vulnerability CAN-2005-0635 CAN-2005-0636	Low/High (High if arbitrary code can be executed)	Security Tracker Alert ID: 1013356, March 2, 2005
GNU 427BB 2.2	A vulnerability exists that could let a remote malicious user conduct Cross-Site Scripting attacks. The 'profile.php' script does not properly validate user-supplied input in the avatar field. No workaround or patch available at time of publishing. A Proof of Concept exploit has been published.	GNU 427BB Input Validation Vulnerabilities CAN-2005-0629	High	Security Tracker Alert ID: 1013337 March 1 2005
GNU CuteNews 1.3.6	Multiple vulnerabilities exist that could let a remote malicious user conduct Cross-Site Scripting attacks or gain elevated privileges. This is due to input validation errors in the 'X-FORWARDED-FOR' and 'CLIENT-IP' variables in '/inc/show.inc.php'. No workaround or patch available at time of publishing. A Proof of Concept exploit has been published.	GNU CuteNews Input Validation Vulnerabilities CAN-2005-0645	High	Security Tracker Alert ID: 1013331, March 1, 2005
GNU Gaim prior to 1.1.4	A vulnerability exists in the processing of HTML that could let a remote malicious user crash the Gaim client. This is due to a NULL pointer dereference. Update to version 1.1.4: http://gaim.sourceforge.net/downloads.php Ubuntu: http://www.ubuntulinux.org/support/documentation/usn/usn-85-1 Fedora:	GNU Gaim Denial of Service Vulnerability CAN-2005-0208	Low	Sourceforge.net Gaim Vulnerability Note, February 24, 2005 **US-CERT VU#795812** **Gentoo, GLSA 200503-03, March 1, 2005** **Mandrakelinux Security Update Advisory, MDKSA-2005:049, March 4, 2005**

	http://download.fedora.redhat.com/pub/fedora/linux/core/updates/ **Gentoo:** **http://security.gentoo.org/glsa/glsa-200503-03.xml** **Mandrake:** **http://www.mandrakesecure.net/en/ftp.php** Currently we are not aware of any exploits for this vulnerability.			
GNU ProjectBB 0.4.5.1	A vulnerability exists that could permit a remote malicious user to inject SQL commands and conduct Cross-Site Scripting attacks. This is due to input validation errors in the 'drivers.php' scripts. No workaround or patch available at time of publishing. A Proof of Concept exploit has been published.	GNU ProjectBB Input Validation Vulnerabilities CAN-2005-0650 CAN-2005-0651	High	Security Tracker Alert ID: 1013332, March 1, 2005
GPL MercuryBoard 1.1.2	Two vulnerabilities exists that can let remote malicious users conduct script insertion and SQL injection attacks. This is due to improper input validation in the avatar URL parameter and the 'f' parameter in 'index.php.' No workaround or patch available at time of publishing. Currently we are not aware of any exploits for these vulnerabilities.	GPL MercuryBoard SQL Injection and Script Insertion Vulnerabilities CAN-2005-0662 CAN-2005-0663	High	Secunia SA14414, March 2, 2005
GPL MyPHP Forum	A vulnerability exists that could permit a remote malicious user to inject SQL commands. This is because several scripts do not properly validate user-supplied input in certain fields. These scripts are: 'forum.php', 'member.php', 'forgot.php', and 'include.php'. **FedoraLegacy: http://download.fedoralegacy.org/redhat/** A Proof of Concept exploit has been published.	GPL MyPHP Forum SQL Injection Vulnerability CAN-2005-0413	High	Security Tracker Alert ID: 1013136, February 9, 200 **Fedora Legacy Update Advisory, FLSA:1748, March 7, 2005**
Hewlett-Packard OpenVMS VAX 6.2-x, 7.3; OpenVMS Alpha 6.2-x, 7.3-1, 7.3-2	A vulnerability exists that could let a local user can gain elevated privileges. HP has issued patches at: http://www2.itrc.hp.com/service/cki/enterService.do Customers who have installed DECnet-Plus must install both MUP kits listed. OpenVMS Alpha V7.3-2 DECnet-Plus MUP - AXP_DNVOSIMUP01-V732.PCSI-DCX_AXPEXE OpenVMS MUP - VMS732_VMSMUP-V0100.PCSI-DCX_AXPEXE OpenVMS Alpha V7.3-1 DECnet-Plus MUP - AXP_DNVOSIMUP01-V731.PCSI-DCX_AXPEXE OpenVMS MUP - VMS731_VMSMUP-V0100.PCSI-DCX_AXPEXE OpenVMS Alpha V6.2-x DECnet-Plus MUP - AXP_DNVOSIMUP01-V63.PCSI-DCX_AXPEXE OpenVMS MUP - ALPVMSMUP01_062.A OpenVMS VAX V7.3 DECnet-Plus MUP - VAX_DNVOSIMUP01-V73.PCSI-DCX_VAXEXE OpenVMS MUP - VAXVMSMUP01_073.A OpenVMS VAX V6.2-x DECnet-Plus MUP - VAX_DNVOSIMUP01-V63 OpenVMS MUP - VAXVMSMUP01_062.A Currently we are not aware of any exploits for this vulnerability.	Hewlett-Packard OpenVMS Access Vulnerability CAN-2005-0652	Medium	HP Security Bulletin HPSBOV01121, SSRT4866 rev.0 March 1, 2005
Jason Hines phpWebLog 0.4.2, 0.5-0.5.3	A vulnerability exists in the 'include_once()' function call due to insufficient sanitization of user-supplied input, which could let a remote malicious user execute arbitrary code. No workaround or patch available at time of publishing. There is no exploit code required, however, a Proof of Concept exploit has been published.	Jason Hines PHPWebLog Remote File Include CAN-2005-0698	High	Security Focus, 12747, March 7, 2005

Mozilla Mozilla 1.7.x and prior Mozilla Firefox 1.x and prior Mozilla Thunderbird 1.x and prior	Multiple vulnerabilities exist in Firefox, Mozilla and Thunderbird. These can be exploited by malicious, local users to perform certain actions on a vulnerable system with escalated privileges and by malicious people to conduct spoofing attacks, disclose and manipulate sensitive information, and potentially compromise a user's system. Firefox: Update to version 1.0.1: http://www.mozilla.org/products/firefox/ Mozilla: The vulnerabilities have been fixed in the CVS repository and will be included in the upcoming 1.7.6 version. Thunderbird: The vulnerabilities have been fixed in the CVS repository and will be included in the upcoming 1.0.1 version. Fedora update for Firefox: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/ **Red Hat:** **http://rhn.redhat.com/errata/RHSA-2005-176.html** **Gentoo:** **http://www.gentoo.org/security/en/glsa/glsa-200503-10.xml** Currently we are not aware of any exploits for these vulnerabilities.	Mozilla / Firefox / Thunderbird Multiple Vulnerabilities CAN-2005-0255 CAN-2005-0584 CAN-2005-0585 CAN-2005-0587 CAN-2005-0588 CAN-2005-0589 CAN-2005-0590 CAN-2005-0592 CAN-2005-0593	High	Mozilla Foundation Security Advisories 2005-14, 15 17, 18, 19, 20, 21, 24, 28 **Red Hat RHSA-2005:176-11, March 1, 2005** **Gentoo, GLSA 200503-10, March 4, 2005**
Mozilla.org Firefox 1.x, 0.x, Mozilla 1.7.x, 1.6, 1.5, 1.4, 1.3, 1.2, 1.1, 1.0, 0.x	A vulnerability exists because a website can inject content into another site's window if the target name of the window is known, which could let a remote malicious user spoof the content of websites **Gentoo:** **http://security.gentoo.org/glsa/glsa-200503-10.xml** A Proof of Concept exploit has been published. Vulnerability has appeared in the press and other public media.	Mozilla Browser and Mozilla Firefox Remote Window Hijacking CAN-2004-1156	Medium	Secunia SA13129, December 8, 2004 **Gentoo Linux Security Advisory GLSA 200503-1** **March 4, 2005**
Mozilla Firefox 1.0	A vulnerability exists in the XPCOM implementation that could let a remote malicious user execute arbitrary code. The exploit can be automated in conjunction with other reported vulnerabilities so no user interaction is required. A fixed version (1.0.1) is available at: http://www.mozilla.org/products/firefox/all.html **Red Hat:** **http://rhn.redhat.com/errata/RHSA-2005-176.html and** **http://rhn.redhat.com/errata/RHSA-2005-277.html** **Gentoo:** **http://www.gentoo.org/security/en/glsa/glsa-200503-10.xml** A Proof of Concept exploit has been published.	Mozilla Firefox Remote Code Execution Vulnerability CAN-2005-0527	High	Security Tracker Alert ID: 1013301, February 25, 2005 **Red Hat RHSA-2005:176-11, March 1, 2005 and RHSA-2005:277-10, March 4, 2005** **Gentoo, GLSA 200503-10, March 4, 2005**
Mozilla Firefox 1.0	There are multiple vulnerabilities in Mozilla Firefox. A remote user may be able to cause a target user to execute arbitrary operating system commands in certain situations or access access content from other windows, including the 'about:config' settings. This is due to a hybrid image vulnerability that allows batch statements to be dragged to the desktop and because tabbed javascript vulnerabilities let remote users access other windows. A fix is available via the CVS repository Fedora: ftp://aix.software.ibm.com/aix/efixes/security/perl58x.tar.Z **Red Hat:** **http://rhn.redhat.com/errata/RHSA-2005-176.html** **Gentoo:** **http://www.gentoo.org/security/en/glsa/glsa-200503-10.xml** A Proof of Concept exploit has been published.	Mozilla Firefox Multiple Vulnerabilities CAN-2005-0230 CAN-2005-0231 CAN-2005-0232	High	Security Tracker Alert ID: 1013108, February 8, 200 Fedora Update Notification, FEDORA-2005-182, February 26, 2005 **Red Hat RHSA-2005:176-11, March 1, 2005** **Gentoo, GLSA 200503-10, March 4, 2005**

Mozilla Mozilla 1.7.3 for Linux, Mozilla 1.7.5 for Windows, and Mozilla Firefox 1.0	A vulnerability exists which can be exploited by malicious people to spoof the source displayed in the Download Dialog box. The problem is that long sub-domains and paths aren't displayed correctly, which therefore can be exploited to obfuscate what is being displayed in the source field of the Download Dialog box. Upgrade available at: http://ftp.mozilla.org/pub/mozilla.org/firefox/releases/1.0.1/source/firefox-1.0.1-source.tar.bz2 Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/3/ **Red Hat:** **http://rhn.redhat.com/errata/RHSA-2005-176.html** **Gentoo:** **http://www.gentoo.org/security/en/glsa/glsa-200503-10.xml** Currently we are not aware of any exploits for this vulnerability.	Mozilla / Mozilla Firefox Download Dialog Source Spoofing **CAN-2005-0585**	Medium	Secunia SA13599, January 4, 2005 Fedora Update Notification, FEDORA-2005-182, February 28, 2005 **Red Hat RHSA-2005:176-11, March 1, 2005** **Gentoo, GLSA 200503-10, March 4, 2005**
Mozilla Mozilla 1.7.3 Mozilla Firefox 1.0 for Windows	A vulnerability exists that could let remote malicious users trick users into downloading malicious files. This is because the the browser uses the different criteria to determine the the file type when saving the downloaded file. Updated versions are available. Mozilla Firefox 1.0.1: http://www.mozilla.org/products/firefox/ Mozilla 1.7.5: http://www.mozilla.org/products/mozilla1.x/ **Red Hat:** **http://rhn.redhat.com/errata/RHSA-2005-176.html** **Gentoo:** **http://www.gentoo.org/security/en/glsa/glsa-200503-10.xml** Currently we are not aware of any exploits for this vulnerability.	Mozilla / Firefox Download Spoofing Vulnerability CAN-2005-0586	Medium	Secunia SA13258, March 1, 2005 Mozilla Foundation Security Advisory 2005-22 **Red Hat RHSA-2005:176-11, March 1, 2005** **Gentoo, GLSA 200503-10, March 4, 2005**
Mozilla Mozilla Firefox 1.0 and 1.0.1	A vulnerability exists that could let remote malicious users conduct Cross-Site Scripting attacks. This is due to missing URI handler validation when dragging an image with a "javascript:" URL to the address bar. No workaround or patch available at time of publishing. **Red Hat:** **http://rhn.redhat.com/errata/RHSA-2005-176.html** **Gentoo:** **http://www.gentoo.org/security/en/glsa/glsa-200503-10.xml** A Proof of Concept exploit has been published.	Mozilla Firefox Image Javascript URI Dragging Cross-Site Scripting Vulnerability CAN-2005-0591	High	Secunia SA14406, March 1, 2005 **Red Hat RHSA-2005:176-11, March 1, 2005** **Gentoo, GLSA 200503-10, March 4, 2005**
Multiple Vendors Multiple (See advisory located at: http://www.uniras.gov.uk/vuls/2004/236929/index.htm for complete list)	A vulnerability exists that affects implementations of the Transmission Control Protocol (TCP) that comply with the Internet Engineering Task Force's (IETF's) Requests For Comments (RFCs) for TCP. The impact of this vulnerability varies by vendor and application but could let a remote malicious user cause a Denial of Service, or allow unauthorized malicious users to inject malicious data into TCP streams. List of updates available at: http://www.uniras.gov.uk/vuls/2004/236929/index.htm NetBSD: ftp://ftp.netbsd.org/pub/NetBSD/security/patches/SA2004-006-kernel/netbsd-1-6/ SCO: ftp://ftp.sco.com/pub/updates/UnixWare/SCOSA-2005.14 ftp://ftp.sco.com/pub/updates/OpenServer/SCOSA-2005.9 SGI:	Multiple Vendor TCP Sequence Number Approximation CAN-2004-0230	Low/High (High if arbitrary code can be executed)	NISCC Vulnerability Advisory, 236929, April 23, 200 VU#415294, http://www.kb.cert.org/vuls/id/415294 TA04-111A, http://www.us-cert.gov/cas/techalerts/TA04-111A.ht SGI Security Advisory, 20040905-01-P, September 28,2004 **SCO Security Advisory, SCOSA-2005.3, March 1 2005**

	http://www.sgi.com/support/security/ **SCO:** **ftp://ftp.sco.com/pub/updates/ OpenServer/SCOSA-2005.3** Proofs of Concept exploits have been published.			
Multiple Vendors OpenPGP	A vulnerability exists that could permit a remote malicious user to conduct an adaptive-chosen-ciphertext attack against OpenPGP's cipher feedback mode. The flaw is due to an ad-hoc integrity check feature in OpenPGP. A solution will be available in the next release of the product. **SUSE:** **ftp://ftp.SUSE.com/pub/SUSE** A Proof of Concept exploit has been published.	Multiple Vendors OpenPGP CFB Mode Vulnerable to Cipher-Text Attack CAN-2005-0366	Medium	US-CERT VU#303094 **SUSE Security Summary Report, SUSE-SR:2005:007, March 4, 2005**
Nokia Nokia Symbian OS	A vulnerability exists that could let a remote malicious user cause a Denial of Service by causing the phone to restart. This is due to a error in the nickname functionality. No workaround or patch available at time of publishing. A Proof of Concept exploit script has been published.	Nokia Symbian OS Phone Denial of Service Vulnerability CAN-2005-0681	Low	Security Focus, Bugtraq ID 12743, March 8, 2005
Oracle Oracle Database Server 8i, 9i	An input validation vulnerability exists in the UTL_FILE package that could let remote malicious authenticated user access arbitrary files on the target system. This is because the of input validation errors is some Directory Object functions. Critical Patch Update - January 2005 is available: http://www.oracle.com/technology/ deploy/security/pdf/cpu-jan-2005_advisory.pdf Currently we are not aware of any exploits for this vulnerability.	Oracle Database Server UTL_FILE Error Discloses Files to Remote Authenticated Users CAN-2005-0701	Medium	Oracle Critical Patch Update, January 2005
PHP Arena paBox	A vulnerability exists that could let a remote malicious user conduct Cross-Site Scripting attacks. A hidden POST variable set to 'text' can trigger the attack. No workaround or patch available at time of publishing. A Proof of Concept exploit has been published.	PHP Arena paBox Cross-Site Scripting Vulnerability CAN-2005-0674	High	Security Tracker Alert ID: 1013363, March 3, 2005
PHP Gift Registry PHP Gift Registry 1.x	A vulnerability exists in 'index.php' due to insufficient sanitization of the 'messageid,' 'shopper,' and 'shopfor' parameters and in 'item.php' due to insufficient sanitization of the 'itemid' parameter, which could let a remote malicious user execute arbitrary SQL commands. **Upgrade available at:** **http://prdownloads.sourceforge.net/ phpgiftreg/phpgiftreg-1.5.0b1.tar.gz?download** Proofs of Concept exploits have been published.	PHP Gift Registry Parameter Input Validation CAN-2005-0292	High	Secunia Advisory, SA13873, January 17, 2005 **Security Focus, 12289, March 7, 2005**
PHP Group PHP 4.0-4.0.7, 4.0.7 RC1-RC3, 4.1 .0-4.1.2, 4.2 .0-4.2.3, 4.3-4.3.8, 5.0 candidate 1-3, 5.0 .0-5.0.2	A vulnerability exists in the 'open_basedir' directory setting due to a failure of the cURL module to properly enforce restrictions, which could let a malicious user obtain sensitive information. Ubuntu: http://security.ubuntu.com/ ubuntu/pool/main/p/php4/ **FedoraLegacy: http://download.fedoralegacy.org /redhat/** There is no exploit code required; however, a Proof of Concept exploit has been published.	PHP cURL Open_Basedir Restriction Bypass CAN-2004-1392	Medium	Security Tracker Alert ID, 1011984, October 28, 200 Ubuntu Security Notice, USN-66-1, January 20, 200 Ubuntu Security Notice, USN-66-2, February 17, 2005 **Fedora Legacy Update Advisory, FLSA:2344, March 7, 2005**

PHP Group PHP 4.3.6-4.3.9, 5.0 candidate 1-canidate 3, 5.0 .0-5.0.2	Multiple vulnerabilities exist: a buffer overflow vulnerability exists in the 'pack()' function, which could let a remote malicious user execute arbitrary code; an integer overflow vulnerability exists in the 'unpack()' function, which could let a remote malicious user obtain sensitive information; a vulnerability exists in 'safe_mode' when executing commands, which could let a remote malicious user bypass the security restrictions; a vulnerability exists in 'safe_mode' combined with certain implementations of 'realpath(),' which could let a remote malicious user bypass security restrictions; a vulnerability exists in 'realpath()' because filenames are truncated; a vulnerability exists in the 'unserialize()' function, which could let a remote malicious user obtain sensitive information or execute arbitrary code; a vulnerability exists in the 'shmop_write()' function, which may result in an attempt to write to an out-of-bounds memory location; a vulnerability exists in the 'addslashes()' function because '\0' if not escaped correctly; a vulnerability exists in the 'exif_read_data()' function when a long sectionname is used, which could let a remote malicious user obtain sensitive information; and a vulnerability exists in 'magic_quotes_gpc,' which could let a remote malicious user obtain sensitive information. Upgrades available at: http://www.php.net/downloads.php Mandrake: http://www.mandrakesecure.net/en/ftp.php Conectiva: ftp://atualizacoes.conectiva.com.br/ RedHat: http://rhn.redhat.com/errata/RHSA-2005-031.html SuSE: ftp://ftp.suse.com/pub/suse/ Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/p/php4/ Apple: http://www.apple.com/support/downloads/ **FedoraLegacy: http://download.fedoralegacy.org/redhat/** There is no exploit code required; however, a Proof of Concept exploit script has been published.	PHP Multiple Remote Vulnerabilities CAN-2004-1018 CAN-2004-1063 CAN-2004-1064 CAN-2004-1019 CAN-2004-1020 CAN-2004-1065	Medium/ High (High if arbitrary code can be executed)	Bugtraq, December 16, 2004 Conectiva Linux Security Announcement, CLA-2005:915, January 13, 2005 Red Hat, Advisory: RHSA-2005:031-08, January 19 2005 SUSE Security Announcement, SUSE-SA:2005:002 January 17, 2005 Ubuntu Security Notice, USN-66-1, January 20, 200 Apple Security Update, APPLE-SA-2005-01-25, January 26, 2005 **Fedora Legacy Update Advisory, FLSA:2344, March 7, 2005**
phpBB Group phpBB 2.0.12	A vulnerability exists that could let a remote malicious user determine the installation path. This is due to improper input validation in the 'highlight' parameter in 'viewtopic.php'. Update to version 2.0.13: http://www.phpbb.com/downloads.php A Proof of Concept exploit has been published.	phpBB 'viewtopic.php' Information Disclosure CAN-2005-0603	Low	[N]eo [S]ecurity [T]eam [NST] - Advisory #06 - 25/02/05
phpBB Group phpBB 2.0.12 and prior	A vulnerability exists that could let a remote malicious user bypass certain security restrictions. This is due to errors in sessiondata['autologinid'], auto_login_key, and viewtopic.php. Update to version 2.0.13. **Gentoo:** **http://security.gentoo.org/glsa/glsa-200503-02.xml** **An exploit script has been published.**	phpBB "autologinid" Security Bypass CAN-2005-0603	Medium	phpBB 2.0.13 Release Notes, February 27, 2005 **Gentoo Linux Security Advisory, GLSA 200503-0 March 1, 2005**
phpBB Group phpBB 2.0.13	A vulnerability exists that could let remote malicious users conduct script insertion attacks. This is because input passed in a signature is not properly validated before being used in 'privmsg.php' and 'viewtopic.php.' No workaround or patch available at time of publishing. Currently we are not aware of any exploits for this vulnerability.	phpBB Signature Script Insertion Vulnerability CAN-2005-0673	High	Secunia SA14475, March 8, 2005
phpBB Group phpBB 2.0.13 and prior	A vulnerability exists in 'oracle.php' that could let a remote user determine the installation path. A remote user can access 'phpBB/db/oracle.php'. No workaround or patch available at time of publishing. A Proof of Concept exploit has been published.	phpBB Group phpBB 'oracle.php' Information Disclosure CAN-2005-0683	Low	[N]eo [S]ecurity [T]eam [NST] - Advisory #09 - 03/03/05

phpBB Group phpBB 2.0.13 and prior	A vulnerability in the 'usercp_register.php' script could let a remote malicious user conduct Cross-Site Scripting attacks. This is due to input validation errors in 'usercp_register.php.' No workaround or patch available at time of publishing. A Proof of Concept exploit has been published.	phpBB Group phpBB 'usercp_register.php' Cross-Site Scripting Vulnerability CAN-2005-0673	High	[N]eo [S]ecurity [T]eam [NST] - Advisory #08 - February 29, 2005
phpMyAdmin phpMyAdmin 2.6.1	Multiple vulnerabilities exist that could let remote malicious users conduct Cross-Site Scripting attacks and disclose sensitive information. This is due to input validation errors in "select_server.lib.php", "display_tbl_links.lib.php", "theme_left.css.php", "theme_right.css.php", "phpmyadmin.css.php", and "database_interface.lib.php." Update to version 2.6.1-pl1: http://sourceforge.net/project/showfiles.php?group_id=23067 **Gentoo:** **http://security.gentoo.org/glsa/glsa-200503-07.xml** **SUSE:** **ftp://ftp.SUSE.com/pub/SUSE** A Proof of Concept exploit script has been published.	phpMyAdmin Cross-Site Scripting and Information Disclosure Vulnerabilities CAN-2005-0543 CAN-2005-0544 CAN-2005-0567	Medium/ High (High if arbitrary code can be executed)	Sourceforge.net, phpMyAdmin Project Tracker 1149383 and 1149381, February 22, 2005 **Gentoo Linux Security Advisory, GLSA 200503-0 March 3, 2005** **SUSE Security Summary Report, SUSE-SR:2005:007, March 4, 2005**
phpMyFAQ Team phpMyFAQ 1.4 and 1.5	A vulnerability exists that could let remote malicious users conduct SQL injection attacks. This is because input passed to the "username" field in forum messages isn't properly validated before being used in a SQL query. Update to version 1.4.7: http://www.phpmyfaq.de/download.php Currently we are not aware of any exploits for this vulnerability.	phpMyFaq SQL Injection Vulnerability CAN-2005-0702	High	phpMyFAQ Security Advisory, March 6, 2005
PHPNews 1.2.4	An include file vulnerability exists that could let a remote malicious user execute arbitrary commands on the target system. This is due to an input validation error in the 'auth.php' script. Update to version 1.2.5: http://newsphp.sourceforge.net/downloads.php Currently we are not aware of any exploits for this vulnerability.	PHPNews 'auth.php' Flaw Permits Remote Code Execution CAN-2005-0632	High	Security Tracker Alert ID: 1013345 March 2, 2005
PhpOutsourcing Zorum 3.5	A vulnerability exists that could let a remote malicious user conduct Cross-Site Scripting attacks or gain elevated privileges. This is due to input validation errors in the 'list', 'method', and 'frommethod' parameters. No workaround or patch available at time of publishing. A Proof of Concept exploit has been published.	PhpOutsourcing Zorum Cross-Site Scripting Vulnerability CAN-2005-0675 CAN-2003-1088 CAN-2005-0676 CAN-2005-0677	High	Security Tracker Alert ID: 1013365, March 4, 2005
PixelApes SafeHTML prior to 1.3.0	A vulnerability exists because the software may not properly filter decimal HTML entities and code containing the \x00 symbol. As a result, remote malicious user could execute arbitrary code. Update to version 1.3.0: http://pixel-apes.com/safehtml/ Currently we are not aware of any exploits for this vulnerability.	PixelApes SafeHTML Remote Code Execution Vulnerability CAN-2005-0648	High	Security Tracker Alert ID: 1013315, February 28, 2005
RealNetworks RealPlayer prior to 6.0.12.1059	A vulnerability in the processing of SMIL files could let a remote malicious user execute arbitrary code. A special Synchronized Multimedia Integration Language (smil) file could trigger to trigger a buffer overflow in the player's SMIL parser. The vulnerability is in 'datatype/smil/renderer/smil1/smlparse.cpp' when processing the screen size attribute. Updates available at: http://service.real.com/help/faq/security/050224_player/EN/ Currently we are not aware of any exploits for this vulnerability.	RealNetworks RealPlayer SMIL Error Permits Remote Code Execution CAN-2005-0455	High	iDEFENSE Security Advisory 03.01.05
RealNetworks RealPlayer prior to 6.0.12.1059	A vulnerability in the processing of WAV files could let a remote malicious user execute arbitrary code. A special WAV file could trigger a buffer overflow and execute arbitrary code. Updates available at: http://service.real.com/help/faq/security/050224_player/EN/	RealNetworks RealPlayer WAV File Error Permits Remote Code Execution	High	RealPlayer Release Notes March 1, 2005

	Currently we are not aware of any exploits for this vulnerability.	CAN-2005-0611		
Smarter Scripts The Includer	A vulnerability exists that could let a remote malicious user execute arbitrary commands on the target system. This is due to input validation errors in the 'includer.cgi' script. No workaround or patch available at time of publishing. A Proof of Concept exploit has been published.	Smarter Scripts The Includer Remote Code Execution Vulnerability CAN-2005-0689	High	Security Focus, Bugtraq ID 12738, March 7, 2005
Squid-cache.org Squid 2.5	A vulnerability exists that could permit a remote malicious user to send multiple Content-length headers with special HTTP requests to corrupt the cache on the Squid server. A patch (squid-2.5.STABLE7-header_parsing.patch) is available at: http://www.squid-cache.org/Versions/v2/2.5/bugs/squid-2.5.STABLE7-header_parsing.patch Conectiva: http://distro.conectiva.com.br/atualizacoes/index.php?id=a&anuncio=000923 Gentoo: http://www.gentoo.org/security/en/glsa/glsa-200502-04.xml Debian: http://www.debian.org/security/2005/dsa-667 Ubuntu: http://www.ubuntulinux.org/support/documentation/usn/usn-77-1 SuSE: ftp://ftp.suse.com/pub/suse/ Trustix: http://www.trustix.org/errata/2005/0003/ Mandrake: http://www.mandrakesecure.net/en/ftp.php RedHat: http://rhn.redhat.com/errata/RHSA-2005-061.html SuSE: ftp://ftp.suse.com/pub/suse/ Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/s/squid/ TurboLinux: ftp://ftp.turbolinux.co.jp/pub/TurboLinux/TurboLinux/ia32/ **Astaro: http://www.astaro.org/showflat.php?Cat=&Number=56136&page=0&view=collapsed&sb=5&o=&fpart=1#56136** **Conectiva: ftp://atualizacoes.conectiva.com.br/** Currently we are not aware of any exploits for this vulnerability.	Squid Error in Parsing HTTP Headers CAN-2005-0174 CAN-2005-0175	Medium	Security Tracker Alert ID, 1012992, January 25, 200 Gentoo GLSA 200502-04, February 2, 2005 Debian DSA-667-1, February 4, 2005 SUSE, SUSE-SR:2005:003, February 4, 2005 US-CERT Vulnerability Note, VU#924198 US-CERT Vulnerability Note, VU#625878 Trustix #2005-0003, February 11, 2005 Ubuntu Security Notice, USN-77-1, February 7, 200 SUSE Security Announcement, SUSE-SA:2005:006 February 10, 2005 Mandrakelinux Security Update Advisory, MDKSA-2005:034, February 11, 2005 RedHat Security Advisory, RHSA-2005:061-19, February 11, 2005 Turbolinux Security Announcement, February 17, 2005 **Security Focus, 12412, March 7, 2005** **Conectiva Linux Security Announcement, CLA-2005:931, March 8, 2005**
Stadtaus Download Center Lite 1.5 and prior	A vulnerability exists that could let remote malicious users include arbitrary files to compromise a vulnerable system. This is due to improper input validation in the "script_root" parameter in "inc/download_center_lite.inc.php". Update to version 1.6: http://www.stadtaus.com/en/php_scripts/download_center_lite/ Currently we are not aware of any exploits for this vulnerability.	Stadtaus Download Center Lite Arbitrary File Inclusion Vulnerability CAN-2005-0680	Medium	Secunia SA14513, March 7, 2005

Stadtaus Tell a Friend Script prior to 2.7	An include file vulnerability was reported in the STADTAUS.com 'Tell a Friend Script' software. A remote user can execute arbitrary commands on the target system. This is because 'inc/tell_a_friend.inc.php' does not properly validate user-supplied input. Update to version 2.7: http://www.stadtaus.com/en/php_scripts/tell_a_friend_script/ Currently we are not aware of any exploits for this vulnerability.	Stadtaus Tell a Friend Script Remote Code Execution Vulnerability CAN-2005-0679	High	SecurityTracker Alert ID: 1013390, March 7, 2005
Stadtaus Form Mail Script 2.3 and prior	A vulnerability exists that could let a remote malicious user execute arbitrary commands on the target system. This is because the 'inc/formmail.inc.php' script does not properly validate user-supplied input in the 'script_root' parameter. No workaround or patch available at time of publishing. A Proof of Concept exploit has been published.	Stadtaus Form Mail Script Lets Remote Users Include and Execute Arbitrary PHP Code CAN-2005-0678	High	Security Focus, Bugtraq ID 12735, March 7, 2005
TYPO3.org TYPO3	An input validation vulnerability was reported in TYPO3. A remote malicious user can inject SQL commands. This is due to input validation errors in the 'category_uid' variable. No workaround or patch available at time of publishing. A Proof of Concept exploit script has been published.	TYPO3 SQL Injection Vulnerability CAN-2005-0658	High	SecurityTracker Alert ID: 1013364, March 3, 2005
Woltlab Burning Board 2.0.3, 2.1.5, 2.2.1, and 2.3.0	A vulnerability exists that could let a remote malicious user inject SQL commands and gain administrative privileges. This is due to input validation errors in the getwbbuserdata() function in the '/acp/lib/session.php' script. Fixed versions (2.0.3pl1, 2.1.5pl1, 2.2.1pl1 and 2.3.0pl1) are available at: http://www.woltlab.info/products/burning_board_lite/index_en.php A Proof of Concept exploit has been published.	Woltlab Burning Board Input Validation Vulnerabilities CAN-2005-0661	High	SecurityTracker Alert ID: 1013351, March 2, 2005
Xerox WorkCentre M35, M45, M55, M165, M175 and WorkCentre Pro 32 Color, 35, 40 Color, 45, 55, 65, 75, 90, 165, 175, C2128, C2636, C3545	A vulnerability exists that could let a remote malicious user gain access to the embedded web server and make changes to the system configuration. This is due to an error in the Web Server component of Xerox WorkCentre printers. A fix is available at: http://www.xerox.com/downloads/usa/en/c/cert_P20_WCP_Patch.zip Currently we are not aware of any exploits for this vulnerability.	Xerox WorkCentre Access Vulnerability CAN-2005-0703	Medium	Xerox Security Bulletin XRX05-005, March 1, 2005

[back to top]

Recent Exploit Scripts/Techniques

The table below contains a sample of exploit scripts and "how to" guides identified during this period. The "Workaround or Patch Available" column indicates if vendors, security vulnerability listservs, or Computer Emergency Response Teams (CERTs) have published workarounds or patches.

Note: At times, scripts/techniques may contain names or content that may be considered offensive.

Date of Script (Reverse Chronological Order)	Script name	Workaround or Patch Available	Script Description
March 8, 2005	ethereal3GA11OverflowExploit.c	No	Exploit for the Ethereal RADIUS Authentication Dissection Buffer Overflow vulnerability.
March 7, 2005	aztek.c	No	Proof of Concept exploit for the Aztek Forum Unauthorized Access Vulnerability.
March 7, 2005	browserDisclose.txt	N/A	Proof of Concept exploit for an information disclosure vulnerability in multiple browsers.
March 7, 2005	chaserfp.zip	No	Exploit for the JoWood Chaser Remote Buffer Overflow vulnerability.
March 7, 2005	FormMailScript_poc.pl	No	Perl script that exploits the Stadtaus.Com PHP Form Mail Script Remote File Include vulnerability.
March 7, 2005	nessuswc-v1.1-02.tar.gz	N/A	NessusWC provides a simple HTTP Web interface to the Nessus Security Scanner.
March 7, 2005	nokia_bt_rr.pl	No	Perl script that exploits the Nokia Series 60 BlueTooth Remote Denial of Service vulnerability.
March 7, 2005	realPlayerSMILFileOverflowPoC.c	Yes	Exploit for the RealPlayer SMIL Error Permits Remote Code Execution vulnerability.
March 7, 2005	weplab-0.1.4.tar.gz	N/A	A tool for reviewing the security of WEP encryption in wireless networks that contains several attacks.

March 7, 2005	Y!PoC.zip	No	A Proof of Concept exploit for the Yahoo! Messenger Offline Mode Status Remote Buffer Overflow vulnerability.
March 5, 2005	calicclnt_getconfig.pm calicserv_getconfig.pm	Yes	Exploits for the Computer Associates License Remote Code Execution Vulnerability.
March 5, 2005	trackercam_phparg_overflow.pm	No	Exploit for the TrackerCam Multiple Remote Vulnerabilities.
March 5, 2005	typo3sql.txt	No	Proof of Concept exploit for the TYPO3 SQL Injection Vulnerability
March 4, 2005	ca3dex.zip	Yes	Exploit for the Ca3DE Multiple Remote Vulnerabilities.
March 4, 2005	phpBBphuket.pl	Yes	Script that exploits the phpBB "autologinid" Security Bypass vulnerability.
March 3, 2005	awstats_shell.c	Yes	Script that exploits the GNU AWStats Multiple Vulnerabilities.
March 3, 2005	CProxyRemote.txt	No	Detailed exploitation for the Computalynx CProxy Directory Traversal & Remote Denial of Service vulnerabilities.
March 3, 2005	ida_sync.zip	N/A	DA Sync was written to allow multiple analysts to synchronize their reverse engineering efforts with IDA Pro in real time.
March 3, 2005	p_wu.c	No	Script that exploits the Wu-FTPD Globbing Denial of Service vulnerability.
March 3, 2005	sb26-2.6.11.tar.gz	N/A	KSB26, Kernel Socks Bouncer for 2.6.x, is a Linux 2.6.x-kernel patch that redirects full tcp connections through a socks5 proxy.
March 2, 2005	foxmail_poc.py foxmail_bof.c foxmail.txt	No	Exploits for the Foxmail USER Command Multiple Remote Vulnerabilities.
March 2, 2005	golden.java	No	Exploit for the Golden FTP Server 'USER" Remote Buffer Overflow vulnerability.
March 2, 2005	trillianPNGOverflow.py trillian.py	No	Exploit for the Cerulean Studios Trillian Insecure Image Data Remote Buffer Overflow vulnerability.
March 1, 2005	cutenews.txt	No	Detailed exploitation for the GNU CuteNews Input Validation Vulnerabilities.

[back to top]

Trends

- On Monday, February 28th, the National Institute of Standards and Technology released the final version of security guidelines designed to protect federal computer systems and the information they hold. The guidelines will serve as a road map for federal agencies in meeting mandates set by the Federal Information Security Management Act (FISA). For more information, see "NIST releases final security guidelines" located at: http://news.com.com/NIST+releases+final+security+guidelines/2100-7348_3-5593256.html?tag=nefd.top
- In a survey conducted by CDW Government, Inc. at the 2005 IPIC conference, federal information technology executives say that cybersecurity is their chief concern. Forty-three percent of federal executives surveyed at a conference this week in Orlando, Fla., said information technology security was their highest priority for 2005. For more information, see " IT executives say cybersecurity is top concern" located at: http://www.govexec.com/dailyfed/0305/030205p1.htm
- When phishing emerged as a serious problem in 2003, many law enforcement agencies were caught off guard. As a result, the FBI and the Secret Service have relied on the private sector for a great deal of help in tracking down phishing sites and taking them offline. For more information, see "Private Sector, Feds Team Up Against Phishing" located at: http://www.eweek.com/article2/0,1759,1772524,00.asp

[back to top]

Viruses/Trojans

Top Ten Virus Threats

A list of high threat viruses, as reported to various anti-virus vendors and virus incident reporting organizations, has been ranked and categorized in the table below. For the purposes of collecting and collating data, infections involving multiple systems at a single location are considered a single infection. It is therefore possible that a virus has infected hundreds of machines but has only been counted once. With the number of viruses that appear each month, it is possible that a new virus will become widely distributed before the next edition of this publication. To limit the possibility of infection, readers are reminded to update their anti-virus packages as soon as updates become available. The table lists the viruses by ranking (number of sites affected), common virus name, type of virus code (i.e., boot, file, macro, multi-partite, script), trends (based on number of infections reported since last week), and approximate date first found.

Rank	Common Name	Type of Code	Trends	Date
1	Bagle.BJ	Win32 Worm	Stable	January 2005
2	Netsky-P	Win32 Worm	Stable	March 2004
3	Zafi-D	Win32 Worm	Stable	December 2004
4	Netsky-Q	Win32 Worm	Stable	March 2004
5	Zafi-B	Win32 Worm	Stable	June 2004
6	Netsky-D	Win32 Worm	Stable	March 2004
7	Netsky-Z	Win32 Worm	Return to Table	April 2004
8	Netsky-B	Win32 Worm	Slight Decrease	February 2004
9	Bagle-AU	Win32 Worm	Slight Decrease	October 2004
10	Bagle.BB	Win32 Worm	Stable	September 2004

Table Updated March 8, 2005

Viruses or Trojans Considered to be a High Level of Threat

- Kelvir.B: Security watchers have warned that the Kelvir.B worm has begun spreading around the world, dropping a payload in the form of another worm, known as Spybot, on infected PCs. The worm spreads using MSN Messenger when unwitting recipients click on a URL in a message reading: "lol! see it! u'll like it" Once clicked the link downloads a variant of the Spybot worm and sends a message to everyone else on the user's contact list. For more information see: http://www.vnunet.com/news/1161784
- Commwarrior-A: The first mobile phone virus capable of replicating via MMS messages has been discovered. Commwarrior-A, which targets Symbian Series 60 phones, is not spreading, but its ability to propagate via Multimedia Messaging Service messages (MMS) worries some experts. For more information see: http://www.theregister.co.uk/2005/03/08/mms_virus/
- Dampig: Virus writers have created a new Trojan capable of infecting Symbian Series 60 smartphones. Dampig-A attempts to trick users into downloading it by posing as the cracked version of the FSCaller application, developed by SymbianWare of Germany. Dampig corrupts the system uninstallation information so it cannot be removed without disinfecting the phone with anti-virus. For more information see: http://www.theregister.co.uk/2005/03/07/dampig_symbian_trojan/

The following table provides, in alphabetical order, a list of new viruses, variations of previously encountered viruses, and Trojans that have been discovered during the period covered by this bulletin. This information has been compiled from the following anti-virus vendors: Sophos, Trend Micro, Symantec, McAfee, Network Associates, Central Command, F-Secure, Kaspersky Labs, MessageLabs, Panda Software, Computer Associates, and The WildList Organization International. Users should keep anti-virus software up to date and should contact their anti-virus vendors to obtain specific information on the Trojans and Trojan variants that anti-virus software detects.

NOTE: At times, viruses and Trojans may contain names or content that may be considered offensive.

Name	Aliases	Type
Backdoor.Binghe		Trojan
Backdoor.Sdbot.AP		Trojan
Commwarrior.A	SymbOS/Commwarrior.A	Symbian OS Worm
Dampig.A	FSCaller SymbOS/Dampig.A	Symbian OS Worm
Downloader-PX		Trojan
Downloader-WJ		Trojan
HackerDefender.sys		Trojan
JS.Trojan.Blinder		Trojan
PWSteal.Bankash.B	Trojan-Dropper.Win32.Agent.fq	Trojan
PWSteal.Bankash.C		Trojan
Skulls.E	SymbOS/Skulls.E	Symbian OS Worm
Spybot.KHO	Backdoor.Win32.Rbot.gen W32.Spybot.KHO	Win32 Worm
StartPage-GN		Win32 Worm
SymbOS.Dampig.A		Symbian OS Worm
SymbOS/Commwarrior.b!sys		Symbian OS Worm
SYMBOS_COMWAR.A		Symbian OS Worm
Tofger.AT	Trj/Tofger.AT	Trojan
Troj/BagleDl-M		Trojan
Troj/Goldun-O	PWS-Banker.k.gen	Trojan
TROJ_BAGLE.BG		Trojan
Trojan.Feutel.B	Backdoor.Win32.G_Door.p	Trojan
Trojan.Flush.A		Win32 Worm
Trojan.Klassir		Trojan
Trojan.StartPage.J		Trojan
VBS.Allem@mm		Visual Basic Worm
VBS/Speery-A	Email-Worm.VBS.Speery.a	Visual Basic Worm
W32.Beagle.BI@mm		Win32 Worm
W32.Beagle.BJ@mm		Win32 Worm
W32.Beagle.BK@mm		Win32 Worm
W32.Comdor.A@mm	Trojan-Downloader.Win32.Delf.jq	Win32 Worm
W32.Gaobot.CPX		Win32 Worm
W32.Kelvir.A	IM-Worm.Kelvir.A IM-Worm.Win32.Kelvir.a Kelvir W32/Kelvir-B WORM_KELVIR.A	Win32 Worm
W32.Kobot.L		Win32 Worm
W32.Serflog.B		Win32 Worm
W32/Agobot-QO	Backdoor.Win32.Agobot.yu WORM_AGOBOT.AKW	Win32 Worm
W32/Bagle.dldr.gen		Win32 Worm
W32/Bropia-G	IM-Worm.Win32.Bropia.n W32/Kelvir.worm.f	Win32 Worm
W32/Flopslene.worm.gen		Visual Basic Worm

W32/Forbot-EP	Backdoor.Win32.Wootbot.gen	Win32 Worm
W32/Forbot-ER	Backdoor.Win32.Wootbot.u	Win32 Worm
W32/Francette-Q	Net-Worm.Win32.Francette.q W32/Kvdbot.worm	Win32 Worm
W32/Kelvir.worm.b	IM-Worm.Win32.Kelvir.a W32.Kelvir.B W32/Kelvir-B WORM_KELVIR.B	Win32 Worm
W32/Kelvir.worm.f		Win32 Worm
W32/Kelvir-B	IM-Worm.Win32.Kelvir.a	Win32 Worm
W32/Kelvir-C	I IM-Worm.Win32 Kelvir.b Kelvir.C W32.Kelvir.C W32/Kelvir-C W32/Kelvir.C.worm W32/Kelvir.worm.c Win32.Kelvir.C WORM_KELVIR.B	Win32 Worm
W32/Kelvir-D	W32.Kelvir.D W32/Kelvir.worm.d Win32.Kelvir.D	Win32 Worm
W32/Myfip-G		Win32 Worm
W32/Myfip-H	Worm.Win32.Myfip.i W32/Myfip.worm.q WORM_MYFIP.G	Win32 Worm
W32/Myfip-H	Myfip.H Worm.Win32.Myfip.h	Win32 Worm
W32/Mytob.gen@MM	Mytob.B Net-Worm.Win32.Mytob Net-Worm.Win32.Mytob.a W32.Mytob W32.Mytob.B@mm W32.Mytob.C@mm W32/Mydoom.bg@MM W32/Mytob W32/Mytob.B@mm Win32.Mytob.C WORM_MYTOB.B	Win32 Worm
W32/Mytob-A		Win32 Worm
W32/Rbot-WV	Backdoor.Win32.Rbot.gen W32/Sdbot.worm.gen.g WORM_RBOT.ASC	Win32 Worm
W32/Rbot-WW		Win32 Worm
W32/Rbot-WX	Backdoor.Win32.IRCBot.y	Win32 Worm
W32/Sdbot.worm!46257		Win32 Worm
W32/Sdbot.worm!78803		Win32 Worm
W32/Sober.O.worm	Sober.O	Win32 Worm
W32/Sober-L	Email-Worm.Win32.Sober.l Sober.L W32.Sober.L@mm W32/Sober-L Win32.Sober.L WORM_SOBER.L	Win32 Worm
W32/Sumom-A	Fatso.A IM-Worm.Sumom.a IM-Worm.Win32.Sumom.a Serflog Sumom.A W32.Serflog.A W32/Assiral.C.worm W32/Crog.worm W32/Fatso.A.worm Win32.Worm.Sumom.A WORM_FATSO.A	Win32 Worm
W32/Tibick-C	P2P-Worm.Win32.Tibick.d W32/Tibick!p2p WORM_TIBICK.A	Win32 Worm
W97M.Sting.B		MS Word Macro Virus
Win32.Bloon.C		Win32 Worm
Win32.Bropia.T		Win32 Worm
Win32.ForBot.MY		Win32 Worm
Win32.Glieder.S		Win32 Worm
Win32.Prutec.I		Win32 Worm

Win32.Tibick.E		Win32 Worm
WORM_BAGLE.BG		Trojan
WORM_ELITPER.B		Trojan
WORM_MYFIP.H	BackDoor-CNX W32.Myfip.R W32/Myfip-G Win32.Myfip.K Worm.Win32.Myfip.gen	Win32 Worm
WORM_RBOT.AQG		Trojan
Zellome	W32.Zellome@m W32/Jeans-A W32/Zellome@M Win32.Shorm WORM_JEANS.A	Win32 Worm

[back to top]

Last updated March 09, 2005